

MAXPRO® Video Management System R670

Installation and Configuration Guide



Installation and Configuration Guide

Honeywell

Revisions

Date	Description
March 8, 2012	New document
February, 2015	Updated for R310 Release
April 2016	Updated for R310 B326 Release
August 2016	Updated for R310 SP1 Release
January 2016	Updated for R400 Release
March 2017	Updated for R410 Release
August, 2017	Updated for R450 Release
November, 2017	Updated for R470 Release
February, 2018	Updated for R490 Release
June, 2018	Updated for R500 Release
September, 2018	Updated for R500 T Patch Release
October, 2018	Updated for R500 SP1 Release
February, 2019	Updated for R550 Release
May, 2019	Updated for R560 Release
November, 2019	Updated for R600 Release
August 2020	Updated for R630 Release
February, 2021	Updated for R670 Release

TABLE OF CONTENTS

Chapter 1 - About this Guide	15
Introducing MAXPRO® VMS.....	15
Scope.....	15
MAXPRO VMS Features.....	16
New Features in R670 Release.....	16
Mask Compliance Detection	16
Social Distancing Violation Detection.....	16
Non-Compliant Social Distancing Regions	16
Analytic Alarms In NVR.....	16
Analytics Tab.....	17
Scalable Analytic Server.....	17
Bulk configurations of cameras from NVR.....	17
Bi-Directional Audio Support for MAXPRO NVR.....	18
Series 60 Camera Integration.....	18
Support for Video Analytics Server - AllGovision	19
IDEMIA Server Integration for FR.....	19
Intelligent Command Support	20
New Features in R630 Release.....	20
Mask Compliance Detection	20
Social Distancing Violation Detection.....	20
Support for Remote Analytics Server.....	21
People Counting Dashboard Utility	21
VMS in VMS support for Mask and Social Distancing Detection.....	21
Faster Drag and Drop for MAXPRO NVR cameras in MAXPRO VMS client ..	21
Series 60 Camera Integration.....	22

Thermal Camera Integration - HRCF-FD384H/HRCF-FD640H	23
New Features in R600 Release	23
New Features in R560 Release	26
New Features in R550 Release	30
Patches Merged in SP1.....	32
Intended Audience	41
Structure of this Guide	42
Typographical Conventions.....	42

Chapter 2 - Commissioning Plan 43

Overview	43
Steps in the Commissioning Process	43
Setting up the Server and Client Computers	43
Installing the MAXPRO VMS R670 Software	44
Securing MAXPRO VMS	44
Configuring the MAXPRO VMS System	45
Verifying the Configuration.....	46

Chapter 3 - Setting up the Client and the Server Computers 47

Overview	47
Before you begin.....	47
Tasks to perform in this phase.....	47
Virtual Machine Specifications	48
Useful Tips	48
Hardware Specifications.....	49
Configuring the Monitor Display Properties	56
About Serial Expander	57
Enabling Windows .NET 3.5	57
NetBIOS Naming Convention Limitations.....	65

Chapter 4 - Installing the MAXPRO VMS R670 Software 67

Overview	67
Before you begin.....	67

System Requirements.....	67
How to Install MAXPRO™ VMS R670	68
Complete Installation	73
Custom Installation	79
Uninstall the MAXPRO VMS R670 Software.....	82
Before you begin	82
After removing MAXPRO VMS.....	89
SQL Express 2014 Sp1 Scenarios.....	91
Cleaning the System	92
Manual Steps if SQL Connection Fails	94
Honeywell Intelligent Command Installation.....	97
Enabling Intelligent Command in VMS.....	97

Chapter 5 - Configuring devices and Setting up a Site99

Overview	99
Before you begin	99
Configuring MAXPRO VMS.....	99
Changing the Default Password.....	101
Setting up a site using Configurator	103
Adding Sites.....	103
Adding Workstations	103
Adding Partitions.....	103
Adding Roles and Users	103
Adding Contact Group and Contacts	103
Adding Event Groups	104
Adding Recorder Groups	104
Adding Serial Ports	104
Adding Analytics	104
Adding Recorders	104
Adding Switchers	104
Adding Video Inputs	105
Adding Video Outputs.....	105
Adding Relays	105
Adding Alarm Inputs.....	105

Adding Logical Cameras	105
Adding Sequences	105
Adding System Macros	105
Adding Joystick Controllers	106
Adding Intercept Keys	106
Scheduling	106
Recorders	106
Adding a Recorder.....	106
Discovering Devices	110
Associating Partitions to the Recorder	114
Events	116
Associating Events and Event Attributes to a Recorder	116
Filtering and Grouping the Recorders	121
Sorting recorder.....	127
Updating a Recorder	129
Deleting a Recorder.....	129
Video Inputs	129
Adding Video Inputs.....	130
Adding a Camera	132
Associating Events and Event Attributes to a Video Input	152
Associating Partitions to Video Inputs	157
Associating Analytics.....	158
Filtering and Grouping the VideoInput(s)	159
Sorting Video Input(s)	164
Updating a Video Input.....	166
Deleting a Video Input.....	166
Adding a Video Input Device.....	167
Adding a Video Input Device (Digital Input Trunk)	167
Video Outputs.....	168
Adding Video Outputs	169
Adding Monitors	171
Adding a Video Output Device	174
Adding a Video Output Device (Trunk)	176
Adding a Video Output Device (Digital Output Trunk)	177

Deleting a Video Output Device	178
Updating a Video Output Device	178
Locking the Display on the Monitor.....	179
Associating Partitions to Video Outputs	179
Associating Video Outputs to Event Groups.....	180
Associating Video Outputs to Joystick Controllers	180
Joystick Controllers	181
Configuring joystick controller.....	181
Connecting the Keyboard to MAXPRO VMS	182
Sign On and Sign Off	182
Configuring the Sign On and Off feature.....	182
Updating a Joystick Controller.....	184
Switchers	186
Adding a Switcher.....	186
Updating a switcher.....	192
Deleting a switcher	192
Associating Partitions to Switcher.....	192
Associating Events to Switcher	193
Relays.....	195
Adding the relay	195
Deleting the Relay	201
Updating the Relay	202
Alarm Inputs.....	202
Deleting the Alarm Input	210
Updating the Alarm Input	211
Contact Group	211
Deleting the Contact Group	213
Updating the Contact group	213
Contacts.....	213
Adding a contact.....	213
Users	215
Adding a User.....	216
Discovering and Importing Users	228
Updating a User	229

Deleting a user	229
Roles.....	230
Adding a role	230
Updating a role.....	240
Deleting a role.....	241
Sequences	241
Creating a Sequence.....	241
Updating a Sequence	244
Deleting a Sequence	244
Analytics	244
Honeywell Video Analytics (ActivEye) Reporting Tool.....	245
Honeywell Video Analytics (ActivEye) Alarm Management	245
Honeywell Video Analytics (ActivEye) Configuration Tool.....	245
Honeywell Video Analytics (ActivEye) Forensics Tool.....	246
Honeywell Video Analytics (ActivEye) live Monitoring Station	246
Honeywell Video Analytics (ActivEye) User Configuration.....	246
Adding an Analytics Server.....	246
Partitions.....	250
Adding a Partition	251
Deleting a Partition	252
Workstations.....	252
Adding a Workstation	252
Deleting a Workstation.....	253
Site	254
Adding a Site	254
Deleting a Site	254
Event Group	255
Adding an Event Group.....	255
Deleting an Event Group.....	256
Intercept Keys.....	256
Adding Intercept Key.....	256
Updating Intercept Keys.....	258
Deleting Intercept Keys.....	258

Logical Camera	258
Adding a Logical Camera	259
Deleting A Logical Camera	261
Updating Logical Cameras	262
System Macros	262
Adding a System Macro	262
Executing a System Macro	263
Deleting a System Macro	264
Recorder Groups	264
Associating recorder to Recorder Groups	264
Disassociating Recorders from the Recorder Groups	266
Updating Recorder Group	267
Deleting Recorder Group	268
Redundancy Controller	269
Configuring Redundancy Controller	269
Disassociating Recorders from the Redundancy Controller	271
Updating Redundancy Controller	271
Deleting Redundancy Controller	272
Redundancy Pool	272
Configuring Redundancy Pool	273
Disassociating Recorders from the Redundancy Pool	275
Updating Redundancy Pool	275
Deleting Redundancy Pool	276
Trinity Controller	277
Serial Port	282
Adding a Serial Port	283
Updating a Serial Port	284
Deleting a Serial Port	286
User Defined Events	286
Failover Constraints	288
Configuring the Failover Constraints	290
Updating Failover Constraints	292
Deleting Failover Constraints	292
Event Association	292

Anonymization	294
Licensing	294
Enabling Anonymization	295
How to configure Anonymization	296
Viewing Anonymized Video	297
Hide Subject Identity	299
Clip Export Option	299
Migration.....	300
Exporting the Files.....	300
Importing the Database	300
Equip Series Camera	302
Scheduler	305
Updating a Scheduler.....	305
Jobs	309
Adding Jobs	309
Alarm Notification	311
SMTP Server Settings	314
Creating an Email Template.....	315
Creating Failover Email Template.....	317
Meta Data Conversion Utility.....	318
Video Analytics Events	324
Manual Archival For Recorders.....	324
Enabling Video on demand feature.....	327
How to Enable/Disable Cameras and Stream.....	328
How to Configure Profile-G or Edge Sync Feature.....	330
Configure the Edge Sync Settings	331
How to Enable Low Bandwidth Streaming.....	335
Enhancing Live Video Streaming in Low Bandwidth Site.....	337
Custom Branding Utility	339
Configuring Multicast.....	342
Four Eye Authentication:	346
How Four Eye Authentication feature Works	348
VMS in VMS Enhancements	350

Default Events Association	351
Enhanced GPU Rendering	353
GPU Rendering Combinations	355
Video Anonymization	356
Playing archived clips through Client machine	358
Annotations	360
Configuring Annotations	360
Enabling Annotations in VMS	361
ADPRO XO Recorder Integration Support.....	366
Export HBOX clip player with clips	367
Playback associated videos for Input Alarms	367
Advanced Rendering Settings	367
SSA - Software Service Agreement for MAXPRO.....	368
People Counting Dashboard Utility	373
VMS in VMS support for Mask and Social Distancing Detection.....	379
Faster Drag and Drop for MAXPRO NVR cameras in MAXPRO VMS client	379
Scalable Analytics Server	380
Bulk configurations of cameras from NVR.....	386
Bi-Directional Audio Support for MAXPRO NVR.....	395
Series 60 Camera Integration.....	397
Allgovision Analytics Box Support	398
IDEMIA Integration with MAXPRO VMS.....	406

Chapter 6 - Verifying the Configuration of MAXPRO VMS..... 415

Overview	415
Before you begin	415
Activities to perform	415
Checking the Connection with VMS server	416
Checking the Device Listing	417
Checking the Live Video from Cameras	418
Checking the Playback of Recorded Video	418
Checking the Bookmark Feature	420
Checking the Playback Loop in Timeline	420

Checking the PTZ Functions	421
Checking for Acknowledgment and Clearing Alarms.....	421
Checking for the Creation of Images	423
Checking the Creation of Clips.....	424
Checking the Sending and Receiving of Operator Messages.....	425
Checking the Surrounding Cameras Feature.....	425
Checking the Saving of Salvo Layout	426
Checking the Device Listing in My Devices	426
Checking the Search for Recorded Video.....	427
Checking the Generation of Reports.....	427

Chapter 7 - Upgrade MAXPRO VMS429

Overview	429
Upgrade to MAXPRO VMS R670.....	429
Upgrade to MAXPRO VMS R630.....	430
Upgrade to MAXPRO VMS R600	431
Upgrade to MAXPRO VMS R560.....	437
Upgrade to MAXPRO VMS R550.....	439
Upgrade To MAXPRO VMS R500 SP1.....	440
Upgrade MAXPRO VMS R500 Build 512 to R500 Build 523.....	442
Upgrade to MAXPRO VMS R500	443
Upgrade MAXPRO VMS R470 Build 476 to R490 Build 495.....	449
Upgrade MAXPRO VMS R410 Build 424 to R470 Build 476.....	451
Upgrade MAXPRO VMS R450 Build 455 to R470 Build 476.....	454
Upgrade MAXPRO VMS R410 Build 424 to R450 Build 455.....	456
Upgrade VMS R410 Build 424 to R450 Build 455 in Korean OS.....	457
Upgrade to MAXPRO VMS R410.....	459
Before you begin.....	460
Upgrade to MAXPRO VMS R410	460
Upgrade MAXPRO VMS R310 to R410 Build 424.....	460
Before you Begin	460
Upgrade MAXPRO VMS R240 To R300.....	467
Upgrade VMS R310 B313 with 3.5 Driver to R310 B326.....	467

Upgrade VMS R310 B 301 with 3.5 Driver to R310 B326	471
Upgrade VMS R310 B 323 to R310 B326.....	472
Upgrade VMS R310 B326 to NVR 4.0 Driver SP1 B 364	472

Chapter 8 - MAXPRO VMS Web Client.....477

Introduction.....	477
Installing Web Client	477
Setting the MAXPRO Web Configurator.....	478
Changing Default Port 443 for Web Client and Mobile App	484
Viewing the Certificate Information	486

This page is intentionally left blank

ABOUT THIS GUIDE

Introducing MAXPRO[®] VMS

MAXPRO[®] Video Management System (MAXPRO[®] VMS) is an enterprise-class video management and hybrid solution. It enables you to perform various surveillance operations on traditional analog, network and IP based video equipment in the same surveillance network. You can deploy thousands of cameras in number of locations, and add many video devices such as recorders and monitors.

Scope

This guide helps you in:

- Setting up the hardware for the MAXPRO VMS system
- Installing and uninstalling the MAXPRO VMS software
- Commissioning the MAXPRO VMS system
- Verifying the MAXPRO VMS system after the commissioning process
- Upgrading from previous versions of MAXPRO VMS to latest versions
- Configure and use MAXPRO Web client
- Install and use MAXPRO Intelligent Command. Refer to the MAXPRO IC User Guide for detailed information on how to use.

MAXPRO VMS Features

The following are the new features in latest MAXPRO VMS release:

New Features in R670 Release

Mask Compliance Detection

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

Social Distancing Violation Detection

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

Non-Compliant Social Distancing Regions

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

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

Analytic Alarms In NVR

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

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

Analytics Tab

In VMS R670 release LPR tab is changed to Analytics tab to display LPR, Facial Recognition and Social Distancing Violation alarms in one place. You can view real time alarms fetched from the Analytics camera and take specific actions on the alarms.

Scalable Analytic Server

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

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

Bulk configurations of cameras from NVR

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

Bi-Directional Audio Support for MAXPRO NVR

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

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

Series 60 Camera Integration

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

Type	Camera Models	Firmware Details
Premium Model	HC60W35R2	Honeywell_L60-Series_IPC_HC60WXXRX_V1.0.21.20200828
	HC60W35R4	
	HC60W45R2	
	HC60W45R4	
	HC60WB5R2	
	HC60WB5R5	
	HC60WZ2E30	
Mainstream Model	HC60W34R2L	
	HC60W34R2	
	HC60W44R2L	
	HC60W44R2	
	HC60WB4R2L	
	HC60WB4R2	
Series60 IR PTZ	HC60WZ5R30	
Series30	HC30W25R3-12V	

Support for Ex-Proof Camera models

MAXPRO VMS R670 supports Ex-Proof Camera integration with MAXPRO NVR 6.7 recorder. The following tables explain the list of supported camera models, Codec and Resolutions supported.

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

Support for Video Analytics Server - AllGovision

MAXPRO R670 released supports Allgovision Analytics Server for non Facial and License Plate Recognition features. The following alarms are supported and displayed in Analytics tab. See [Allgovision Analytics Box Support](#) section how to configure and view these alarms.

Alarms	Alarms	Alarms
Trespass	Vehicle Counting	Safety Gear Detection
Loitering	Wrong Way Detection	Jaywalking
Tripwire	Over speeding Detection	Pedestrian Counting
Left Object Detection	Traffic Signal Detection	Pedestrian Dwell Time
People Counting	License Plate Recognition	Yellow Box Violation
Camera Tampering	License Plate Detection	Illegal Lane Change
Missing Object Detection	Vehicle Halt Detection	Wrong Lane Violation
Illegal Parking	Speed Drop Detection	No Flame Detection
Vehicle Congestion	Face Recognition	Social Distancing Violation
Tailgating	Auto PTZ Tracking	No Mask Detection
Crowd Detection	Graffiti Detection	Accident Detection
Counter Flow	Garbage Detection	
Video Smoke Detection	Video Loss Alarm	
Fire Detection	Slot Based Parking Management	
Slip and Fall Detection	Fog Detection	
Face Detection	Gesture Recognition	
Queue Management	Crowd Behavior Analysis	

IDEMIA Server Integration for FR

IDEMIA server allows you to Integrate the VMS/NVR and Cameras with Facial Recognition based analytics server for leveraging the facial recognition and analytics capability (ability to blacklist/white-list). This server handles the FR based analytics alarms/events on the VMS thick client. Also integrates the additional analytics events of IDEMIA in Analytics tab. See [IDEMIA Integration with MAXPRO VMS](#) section for more information on how to configure and view the alarms in VMS.

User can perform the following:

- Monitor FR analytics server alarms MAXPRO VMS Analytics tab
- Enable/disable alarms per FR Analytics server
- Access the details related to Analytics server
- View Bounding boxes on the analytics tab for the events coming in.
- Acknowledge events coming into the analytics tab
- Search the events with description or confidence score and filter based on specific analytics type
- View the associated clip with the event

- View additional analytics events from IDEMIA
- Real-time alert based on face/body /clothing identification
- Crowd analysis
- Intrusion detection
- Person and object counting

Intelligent Command Support

MAXPRO Intelligent Command is a common user interface that provides valuable enhancements to security systems. These ensure compliance with stringent industry regulations. For instance, Intelligent Command enables operators to respond rapidly and effectively to alarms or incidents by providing a Standard Operating Procedure (SOP) that shows the process that should be followed. This reduces both compliance exceptions and security risks.

The MAXPRO interface gives users a stronger situational awareness of the whole security system through a single map view of all the access, video and intrusions solutions. Refer IC User Guide for detailed information.

New Features in R630 Release

Mask Compliance Detection

Mask Compliance Detection feature detects the people who are with and without Masks in a given scene. This feature detects in a real time scenario and generates an event for People with/without mask. It helps in monitoring the people those who are violating the compliance of not wearing a mask in public places. This feature requires dedicated license to configure and use. Refer to the MAXPRO VMS 630 Operators Guide on how to configure and use this feature.

Social Distancing Violation Detection

Social Distancing Violation detection feature detects distance between two people and raises an alarm if the social distance norm is violated. This feature helps to ensure social distancing is followed in your premises. This feature requires dedicated license to configure and use. Refer to the MAXPRO VMS 630 Operators Guide on how to configure and use this feature.

Alarms for both Mask Detection and Social Distancing

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

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

Operating Conditions

There are various recommendation with respect to operating conditions for both Mask Detection and Social Distancing to give good results. It is recommended to refer these operating conditions before using these feature. Refer to the MAXPRO NVR 630 Operators Guide for more information.

Support for Remote Analytics Server

MAXPRO R630 released support for Remote analytics Server configuration for Mask and Social Distancing on i8700 Machines. This configuration is required if the existing systems are not capable to take up the load of Analytics and to avoid overshoot of CPU memory.

People Counting Dashboard Utility

VMS Occupancy Dashboard Utility allows you to track the number of people entered or exited from a specific area or premises or pathway. This utility helps to manage the space in commercial buildings to take appropriate actions based on the number of people entered or exited. The Occupancy Dashboard displays the Occupancy Summary and Trend based on the cameras configured and duration. This utility needs to be used along with MAXPRO VMS and HVA.

The actions are:

- Monitoring/Managing parking area/building
- Space management in big stadiums/shopping mall

See [People Counting Dashboard Utility](#) section for more information on configuration.

VMS in VMS support for Mask and Social Distancing Detection

MAXPRO VMS R630 release supports Mask and Social Distancing Violation Detection support for VMS in VMS scenario with Bounding boxes. User can view bounding boxes in both Master and Child VMS recorders. This enhancement allows user to track the Mask and Social Distancing alarms and events in a wide range of recorders

For Master VMS both Alarm and events along with attributes are supported. For Child VMS attributes are not supported.

User need to enable View Annotations in Preference dialog box after configuring VMS in VMS.

Faster Drag and Drop for MAXPRO NVR cameras in MAXPRO VMS client

The time taken for the video to render in VMS client after drag and drop on to the video panel has been considerably improved. This feature requires a configuration to be enabled.

To enable this feature user need to configure the values in config files based on 32/64 bit rendering modes. See [Faster Drag and Drop for MAXPRO NVR cameras in MAXPRO VMS client](#) on how to configure.

Series 60 Camera Integration

MAXPRO VMS R630 supports Series 60 Camera integration with MAXPRO NVR 6.3 recorder. The following tables explain the list of supported camera models, and events/alarms supported.

Type	Camera Models	Firmware Details
Premium Model	HC60W35R2	Honeywell_L60-Series_IPC_HC60WXXRX_V1.0.20.20200814 Note: If a camera has older firmware, please upgrade to this version or above and perform factory default once before upgrade
	HC60W35R4	
	HC60W45R2	
	HC60W45R4	
	HC60WB5R2	
	HC60WB5R5	
	HC60WZ2E30	
Mainstream Model	HC60W34R2L	
	HC60W34R2	
	HC60W44R2L	
	HC60W44R2	
	HC60WB4R2L	
	HC60WB4R2	

Supported Events/Alarms

Series 60 Camera models support the following events/alarms:

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

Supported key Features

- HTTPS integration: The camera supports complete HTTPS protocol while integrating with NVR.
- Smart Stream III
 - Smart Codec
 - Smart FPS

- Dynamic intra Frame Period (DIF)
- Alarms
- Profile S compliant
- Multicast
- Edge Sync Recording Support
- Full Encrypted Communication (including Encrypted Profile G communication)

Thermal Camera Integration - HRCF-FD384H/HRCF-FD640H

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

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

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

New Features in R600 Release

SSA - Software Service Agreement for MAXPRO

Software Service Agreement (SSA) is a flexible version specific licensing process which allows a user to get the support on the MAXPRO VMS licenses across multiple versions. From R600 release user need to buy a valid license to upgrade or for fresh installation. In addition, user can buy SSA support license for a specific duration which helps to get support from Honeywell.

Please contact Honeywell Customer support. See the back cover for the contact information in respective regions.

License Plate Recognition (LPR)

Enhancements has been made in LPR feature to support events with cropped images, categorization and details pane. LPR scans can be monitored through a dedicated window in MAXPRO thick client. This new windows also supports filtering and searching events based on camera and category (White/Black listed/unknown).In addition you can also view the specific event video from the LPR feed.

NDA Series 30 camera Integration in MAXPRO NVR & VMS

Series 30 Camera integration is supported in R600 release with MAXPRO NVR recorder. The following tables explain the list of supported camera models, firmware version and events.

Note: HC30WF5R1 model camera does not support HTTPS.

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

Supported Events

Series 30 Camera models support the following events:

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

Supported key Features

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

- Profile S compliant
- Multicast

Secure video communication with Series 30 Cameras

Refer to the 800-25609-A_Honeywell 30 Series IP Cameras Network Security Guide for complete details.

MPEG2 Encoder Support with MAXPRO NVR and VMS

R600 supports legacy MPEG2 Encoders with Live and playback, Alarms and VMS in VMS functionalities. The following encoders are supported.

- ENC8M2
- VE8M2

Supported Firmware Version: 1.2.261

Supported Features are:

- Alarms
- VMS in VMS
- Live
- Playback
- Export
- Only Multi casting streaming address

User Experience Improvements in MAXPRO VMS Thick Client

A complete user interface reskin (Black theme) for MAXPRO VMS thick client with improved user experience is implemented in R600 release.

This includes the following:

- Main Panels
- Left Panel
- Calendar look and feel
- Alarm flashing: Controlled on Thick client using config file
- Clip buttons
- Icons
- Docking controls
- Utility Drop-down, Digital correction and Create Salvo window
- Preferences drop-down, preferences window and all popup windows
- About box
- Clip Export window and clip export status window

- License window

Recorders Supported

Following are the default supported recorders for R600. Other recorders are not part of the installation. Please contact Honeywell Tech support team for support. See the back cover for contact information.

- MAXPRO NVR
- Performance Series Embedded NVR
- ADPRO XO
- VMS in VMS

Video Guard service for SIRA compliance

MAXPRO R600 release supports SIRA compliance with Video Guard Agent. This is to meet the specifications defined as part of the City wide Surveillance initiative by the Security Industry Regulatory Agency (SIRA) of Dubai, UAE, and being adopted across Middle-East countries

New Features in R560 Release

Smooth Reverse Playback

This is an enhancement to the existing reverse playback feature in MAXPRO VMS and it is recommended for the sites with lower GOP settings. Smooth reverse playback allows user to view the reverse playback operation without any jerk in the playback video. Depending on the FPS and GOP setting in NVR camera properties, smooth playback video is displayed. Its is recommended to set the GOP value in the range of 5 to 10 to experience smooth reverse. This helps to view the best in class playback video during site monitoring and investigation without dropping video frames. This enhancement is supported only with MAXPRO®NVR recorder and user can enable this option in MAXPRO VMS > Preferences tab. Refer to the [MAXPRO® VMS Operators Guide](#) on how to enable and use this feature. User can perform and experience the following reverse playback functions smoothly.

Note: *For smooth reverse playback, it is recommended to use lower GOPs (i.e less than FPS. For Example: 30FPS/5GOP, 30/10,10/10 and so on)*

- Smooth playback in reverse direction for speeds upto 2x
- Key frame reverse playback at 4x, 8x and 16x speed
- Reverse playback on slow speed (1/8x to 1/2x)
- Reverse playback for multiple cameras
- Reverse playback for multiple cameras in Sync mode (Sync playback)
- Step reverse for cameras (frame-by-frame)

Enhanced Inter NVR Sync playback

Inter recorder sync playback for cameras across MAXPRO NVR is improved from previous releases. Inter NVR sync playback features helps user to synchronize the playback video feed across multiple cameras and recorders. In R560 release user can experience sync playback with both forward and reverse direction with high speeds (and smooth playback upto 2x speed). User can also perform other operations such as step reverse and step forward in sync playback mode and can view smooth video. This feature is supported with MAXPRO NVR and Enterprise recorders only.

Note: It is recommended to remove camera loops before performing Sync Playback.

Support for Equip-S Series V2 Cameras

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

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

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

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

Camera Model	Firmware	Web Version	Onvif Version	ISOM Version	Xtralis Intrusion Trace	Xtralis loitering Trace	Intrusion Detection	Loitering Detection	Trigger Line Detection
Equip S Series V2 Firmware version					VA Packages				

Low Light	1.000000 00.18, 2019-04- 23 Or above	3.2.1.72 2805	16.1.2	1.3.1, 2019- 04-21	1.01.19	1.01.19	1.0.8, 2019-01- 15	1.0.8, 2019-01- 15	1.0.8 2019- 01-15
WDR cameras	1.000000 00.18, 2019-04- 09 Or above	3.2.1.71 6054	16.1.2	1.3.1, 2019- 04-04					

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

- New VA events added with Annotation support
 - Xtralis IntrusionTrace™
 - Xtralis LoiterTrace™
 - Intrusion Detection
 - Loitering Detection
 - Trigger Line Detection

Note: Annotation feature is supported only with Xtralis XO packages.

- Profile -G Edge Sync recording
- Multicast

Introduced Advanced Rendering settings

This feature provides flexibility to select different rendering combinations between CPU and GPU modes for decompression and rendering process. Earlier only GPU Rendering capability was available to handle the camera video packets along with decompression. With Advance Rendering settings user can choose to distribute the load on CPU and GPU accordingly. This helps the user to improve the rendering performance of the system. Refer to the [MAXPRO® VMS Operators Guide](#).

- CPU Decompress + CPU Render: This option executes low performance because entire video rendering process will be on CPU. This option is for debugging purpose and is recommended not to be selected.
- GPU Decompress + CPU Render: By default this option is selected and decompression/rendering process is shared between GPU and CPU.
- GPU Decompress + GPU Render: This option is for high resolution cameras and for cameras with 60 FPS on 4K monitors. Selecting this option may reduce the number of cameras but the video quality will be best.

Note: GPU Decompress + GPU Render option has some limitations such as Flip/Mirror/Digital corrections features may not be supported.

Change in UI Naming Convention

- In Preferences dialog box:

- Enabled GPU Rendering is now renamed as Support 64 Bit Rendering with more granular control with advanced rendering options.
- Set FPS Limit for Unselected Panel is now renamed as Switch to I Frames for unselected panels.







Enhancements in ADPRO XO Recorder

- Export HBOX clip player with clips: MAXPRO VMS integration with ADPRO XO recorder allows user to export clip (HBOX format) along with the HBOX clip player. This helps the user to play the clip in any machine without depending on supported clip format player. Refer to the [MAXPRO® VMS Operators Guide](#) on how to export a clip.
- Capability to playback associated videos for Input Alarms: This feature enables user to playback the associated video with input alarm. User can view the video for an input alarm from all the associated cameras. This feature is support only from ADPRO XO recorder integration with VMS. Refer to the [MAXPRO® VMS Operators Guide](#) on how to view the videos of input alarms.



Enhancements in Time line color in Viewer

Timeline in Viewer tab is improvised to identify various recordings using colors. Based on the legends user can identify recordings such as Continuous, Event, User based, Archival and Failover. The following are the various timeline indicators introduced.

For Recording

Color	Indicates...
	Continuous recording.
	Event based recording.
	User based recording.
	On Device
	Synced From Device
	Redundant

For Archival

Color	Indicates...
	Archival of Continuous recording
	Archival of Event based recording

Enhancements in VMS in VMS Discovery

VMS in VMS discovery will now help to discover and add sites with same IDs (under different Child VMS) in order to maintain the logical grouping of cameras in Master VMS. Consider an example as explained below:

Example Scenario:

- CameraA of Site1 (Site ID 1) in VMSA
- CameraB of Site1 (Site ID 1) in VMSB

Before R560:

- After VMS in VMS discovery: Both VMSA and VMSB is displayed in “Master VMS”. CameraA and CameraB displayed in Site1 of “Master VMS”

After R560:

- After VMS in VMS discovery:
 - CameraA will appear under Site1 in “Master VMS”
 - CameraB will appear under Site1_VMSB in “Master VMS”

New Features in R550 Release

Edge Analytics Annotation Support

Annotations support for Intrusion Trace and Loiter Trace in Live and Playback video is supported in MAXPRO® VMS with MAXPRO® NVR recorder integration. This feature helps to trace and locate the moving subjects in live/recorded video and generates an alarm if intrusion or loitering is detected.

Equip-S series camera supports Annotation feature along with Intrusion trace and Loitering Trace alarms. These alarms are in-built with Equip-S series camera and are made available by installing required analytics licenses.

See [Annotations](#) section for more information.

ADPRO XO Recorder Integration Support

ADPRO XO Recorder is integrated with MAXPRO VMS in R550. In MAXPRO VMS user can also see the Annotation bounding boxes with XO recorder integration. User needs to update new license to avail the features of XO recorder in VMS.

Note: Honeywell recommends you to change the default username and password after the first login.

The following are the qualified XO Recorder models and the Firmware versions supported with MAXPRO VMS R550

.

#	XO Recorder Model (Version)	Firmware Version
1	ADPRO IFT	IFT
		IFTE
2	Fast Trace 2	XO 04.02.0010
3	ADPRO IFT Gateway	XO 04.02.0012

Following are the features supported with ADPRO XO Recorder integration.

:

#	Features Supported
1	Add/delete/modify AdproXO recorder in VMS
2	Discover Cameras, Relays and Sensors
3	Live Video
4	Multi Stream
5	Snapshot save, digital correction, Mirror and Flip.
6	PTZ operations
7	Playback Operations Note: Reverse playback operation is not supported. Playback operation may start a few seconds behind the selected time because of GOP settings.
8	Camera Status/Alarms
9	Events Search
10	Anonymization
11	HVA

Patches Merged in SP1

5.0 T Patch

- Refer to the 800-23558-E_MAXPRO™ VMS R500 SRB T-Patch for complete information on new features in R500 T Patch.

Windows Expiry Patch

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

Include Archived Clips

This feature allows user to search Archived clips including the recording clips. User needs to select Include Archived Clips check box under Filter area while searching for recorded clips. Based on the search criteria the archived clips are displayed in Grey color as shown below. When user drag and drop the archived clips in to the panel then camera name and clips status is displayed. Refer to [MAXPRO® VMS Operators Guide](#) for more information on how to search for archived clips.

To play the Archived clips through a client machine, see [Playing archived clips through Client machine](#) section.

Primary and Archived Location

The location of Archived clips is now displayed in the Result windows in Location column as highlighted below. The type of status is explained below.

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

Camera Name & Clip status

In Viewer screen following are the improvements:

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

Improved GPU rendering

GPU Rendering capability is now enhanced to handle camera video packets along with decompression technique. User can view smooth and clear live video through GPU rendering. User should modify the registry value in client or server machine to enable GPU rendering mode. See [Enhanced GPU Rendering](#) on page 353 to experience the improved GPU rendering mode.

GPU Rendering Combinations

The below table explains the combination settings between Enable GPU Rendering option and Registry settings

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

60FPS support for EQUIP-S 1080P cameras

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

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

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

Video Anonymization Environment selection options

This feature allows you to configure or mask identifiable objects based on the scene environment. User need to select the required environment from the drop down list based on the camera mounting position. See [How to Anonymize objects based on Environment](#) on page 356 for more information.

The following are the Environments supported in this T-Patch

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

New Column for Anonymization in Video Inputs

A additional column Anonymization in Video Inputs screen is introduced to view the list of camera associated/configured with anonymization feature. User can also apply filter True/False to view the list of cameras associated, where True is associated camera and False is not associated.

Platform Refresh: R500 Installation is supported on Windows 2016 Operating systems (Server)

Privacy Protection Settings (GDPR)

1. Anonymization Support: Anonymization feature is to help the business owner to meet the EU GDPR compliance standards easily. The objective of this feature is to hide the identifiable personal data or personal identity in a video surveillance system using masking techniques. This feature is specific to European Union region. MAXPRO VMS R500 release enables user to configure and experience this feature. The configuration can be done in Configurator tab and only an Administrator can use this feature and grant access. EquipIP Series cameras supports this feature and user can associate the required cameras to anonymize. Anonymization is also implemented on HVA streams.

The Anonymization feature supports the following type of masking:

- Blur: Blurs the Identifiable object
- Pixelize: Pixelizes the Identifiable object

Note: This feature is license based and it is not supported in Viewer Edition. In R500 Enterprise Edition for both (GDPR) features, 60 days trial license is enabled. For R500 Viewer Edition these features are not available in the permanent demo license.

- New User Privilege: Introduced new user privilege “Hide Subject Identity” to control the accessibility to view Anonymized video. An Administrator can decide to enable this option to hide the subject identity for a specific Operator. By default this check is enabled for all the operators.

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

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

2. Four Eye Authentication: This feature is also part of Privacy Protection setting and to meet the EU GDPR compliance standards easily. This is to restrict all users in a surveillance system to perform Playback operation. While performing playback operation at least two people from different roles should authenticate. For an Administrator, authentication is not required and can perform any playback operation. However, using license; authentication for an administrator can be configured.
For a non Administrator user, by default a pop up is displayed and an Administrator user or a User from some other group needs to authenticate to perform playback operation.

Note: This feature is license based and it is not supported in Viewer Edition. For R500 Enterprise Edition 60 days of trial license is applicable for both (GDPR) features. For R500 Viewer Edition these features are not available in the permanent demo license.

The following table explains the Four eye authentication based on the user and roles.

User	Authenticating User	Valid Authentication
User 1 [of Group 1]	User 1 [of Group 2]	Yes
User 1 [of Group 1]	User 2 [of Group 1]	No

I18N Localization Support:

- I18N support includes new strings from R410 to R490 and in MAXPRO VMS R500 release additional Turkish Language is supported.

VMS in VMS Enhancements:

- Apart from cameras, relays and sensors, user can now discover sites, workstations, partitions and users from child VMS. This feature helps user to import the configurations instead of reconfiguring and in turn saves time for Large scale deployments.

Extended Salvo layouts

- Additional 5X5, 6X6, 7X7 and 8X8 salvo layout combinations are introduced in this release to reduce the cost involved in monitors.

Default Events Association

- After upgrading to R500, if user discovers the recorders then for only newly added recorders, by default all the events will not get associated to cameras.

Only few events will be associated with the devices and cameras. The following are the list of events associated by default. If user need more events to be associated then it needs to be configured manually. See [Associating Events and Event Attributes to a Recorder](#) on page 116 for more information.

#	Event Name
1	CAMERA_VIDEO_LOSS
2	CAMERA_DISABLED
3	CAMERA_ENABLED
4	DISCONNECTED
5	CONNECTED
6	CAMERA_DELETED
7	CAMERA_ADDED
8	CAMERA_VIDEOLOSS_ALARM
9	CAMERA_VIDEOLOSS_CONFIGURATIONFAILED
10	CAMERA_VIDEOLOSS_CONFIGURATIONOK
11	CAMERA_VIDEOLOSS_OK
12	CONNECTION_LOST
13	OFFLINE
14	VIDEO_LOST
15	VIDEO_RESTORED

New Equip 1080p and 4MP Camera Integration

- Configuration is done through Honeywell proprietary ISOM APIs
- After integrating the new Equip Camera, system will be able to support the following
 - H.264, H.265 and MJPEG coded support
 - HTTPS support
- New events supported: Equip series Camera integration generates the following additional events.
 - Abandoned Object detection
 - Object Missing detected
 - Trigger Line detection

The following Equip series camera models are supported using ISOM API's

#	Camera Model	Description	Firmware Version Details
1	H4L2GR1V	2MP Lowlight outdoor dome	Version: 1.000.0000.10, Build Date: 2018-05-29 ISOM Version 1.2.1_Build 20180529 VA Package Version: 1.0.8_build20180529
2	HBL2GR1V	2MP Lowlight IR bullet	
3	HCL2GV	2MP Lowlight box camera	
4	H4W2GR1V	2MP WDR outdoor dome	Version: 1.000.0000.9, Build Date: 2018-05-25 ISOM Version: V 1.2.1_Build 20180524
5	H4W4GR1V	4MP WDR outdoor dome	
6	HBW2GR1V	2MP WDR bullet, 2.7-13.5mm	
7	HBW2GR3V	2MP WDR bullet, 5-60mm	
8	H3W2GR1V	2MP WDR indoor dome	
9	H3W4GR1V	4MP WDR indoor dome	
10	HCW2GV	2MP WDR box camera	
11	H2W2GR1	2MP Pancake camera	

Multicast Support

Allows you to view the Live video continuously in VMS clients despite of any interruption in NVR recorders. Previously without Multicast, only one camera can see only 16 times now this limit is broken. User can view live video in N number of clients. However, the camera should be Multicast capable. Multicast cameras should be accessed from client network and only Equip-S model cameras are supported. Ensure that Multicast is enabled in the Network switch. See [Configuring Multicast](#) section for more information.

Enhancements in Network Throttling

Depending on the available network bandwidth at site, for better user experience and to improve the performance of Live video streaming, user needs to manually configure the config file and the Registry Entries. See [Enhancing Live Video Streaming in Low Bandwidth Site](#) for more information on how to configure.

Custom Branding Utility

A distributable utility to customize the brand parameters of a business organization is introduced. User can contact to Honeywell Dealer or Tech support to obtain this utility. Please see the back cover for contact information.

Global Bookmarks

Bookmarks tab is included in Viewer to create bookmarks on a live video and save under the bookmarks tab. This window and options are displayed based on the user privileges. User can Create Bookmarks, Play video from Bookmarks time, send operator and monitor messages to the user and configure the bookmark retain and recycle settings in Preference > Bookmarks Settings tab.

Third Party ONVIF Profile G supported cameras:

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

Profile G Cameras	Camera Type	Firmware Details
Tyco	ADCi350-B111	V3.1.0.170215
Samsung	QNO-7010R	1.04_170224
Panasonic	WV-SFV631L	2.41

MAXPRO Web Configurator

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

Network Throttling Options

Introduced the following options for better management of resolution and frames. This feature automatically measures the latency in streams periodically and manages the stream with lower resolution and lower frame rate in low network bandwidth sites. This enables user to view smooth video without fluctuations. This feature is applicable for Live streaming only.

- Mange Resolution
- Manage Frames

Rendering Options

- Show Stream Details: Allows you to view the stream details such as type of camera Resolution, FPS on the video panel.

Inter-NVR Sync playback

Enhancements made in Inter NVR Sync Playback feature, where user can sync the playback video across MAXPRO NVR recorders. This feature is supported from R450 release and only supported for MAXPRO NVR.

On Demand live Streaming (VOD)

On Demand live Streaming (VOD): On Demand Live Streaming / recording feature enables you to configure and store recordings at camera level. This feature saves the bandwidth for remote sites with limited and costly connectivity (e.g. using 4G). MAXPRO NVR configured as On Demand Live Streamer will stream video from cameras only. Later when a client requests a live stream for viewing, the recordings at the camera level can be synced back to view in NVR viewer. VOD is used to pull video streams only when you want the stream for viewing or analysis (such as Smart VMD, HVA Analytics in VMS and so on). When this feature is enabled, recording will not take place in MAXPRO NVR. This feature is compatible from MAXPRO NVR Viewer, MAXPRO NVR Web Clients and MAXPRO NVR Mobile app clients.

Profile-G or Edge Sync Support:

Allows you to synchronize the recordings from the camera SD card to NVR. This feature enables the user to playback only those recording which are saved on demand in the SD card. Flexibility to enable the Edge sync in Camera page and configure the day/ time for Edge Sync Settings in System window to get the recordings from the camera. This feature is supported only for equip 1080p WDR, 4MP WDR and IR PTZ model cameras.

H.265 Codec GPU Rendering Support

H.265 codec cameras now supports GPU based Rendering. You can render upto 23 H.265 cameras with 1080P Resolution at 30 FPS/30 GOP. Refer MAXPRO NVR Desktop Client - Workstation Specifications and Performance Metrics for more information.

Low bandwidth Stream Settings:

Use Low Resolution Stream

This feature is for low bandwidth sites and to view the low resolution video in any size of salvo layout. User needs to configure the low resolution for any stream in NVR camera page. Select the Low Resolution check box in VMS > Preference > Advanced Settings tab, to view the low resolution video in single or multiple salvo layout.

Note: Either you can select the Enable Switch Stream feature or Use Low Resolution stream feature.

Receive Only I Frame/Low Bandwidth Streaming

This feature allows user to receive and view only I Frame considering the bandwidth at the site. User needs configure the low resolution and choose to render only I Frame in NVR. This enables user to view the required clips even with low bandwidth.

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 current video panel size. 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. User needs to configure the Primary and secondary streams with high or low resolutions or vice versa in MAXPRO NVR camera page. Based on the configuration, user can drag and drop the camera in VMS, in single or multiple salvos.

Note: *Either you can select the Enable Switch Stream feature or Use Low Resolution stream.*

Manual Archival support for Primary and Redundant Recorders-

Manual Archival feature enables you to manually Archive the clips of both Primary and Redundant Recorders. You can search the required recording clips in Search tab and then archive. Before performing the manual archive ensure that you configure the Drive path in NVR and then map the Archival storage drive path in VMS > Viewer tab.

Embedded NVR Recorder (Embedded Recorder) Support

User can configure and use the Embedded Recorder features in MAXPRO VMS 450 and later versions. Refer to the latest [MAXPRO® VMS SRB Document](#) for the list of features supported.

New EquiP Series Camera Models Support

Additional 8 new EquiP camera models are now supported (HFD6GR1, HSW2G1, HCD8G, HBD8GR1, H4D8GR1, HDZ302DE, HDZ302D, HDZ302DIN) in MAXPRO NVR 4.1 and the same can be accessible in MAXPRO VMS R410. 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

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. If the camera is added in NVR box then you can perform 3D positioning in MAXPRO VMS. Refer to the [MAXPRO® VMS Operators Guide](#) for various views for how to use 3D Positioning.

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. User needs to configure this feature in NVR box. Refer to the [MAXPRO® VMS Operators Guide](#) for various views of EquiP camera.

H.265 Codec Support

H265 codec type is supported to optimize the storage requirements for higher resolution cameras. H265 is only supported for New EquiP model cameras. (HFD6GR1, HSW2G1, HCD8G, HBD8GR1, H4D8GR1, HDZ302DE, HDZ302D and HDZ302DIN). You can view these higher resolution cameras in MAXPRO VMS R410 if it is added in MAXPRO NVR box.

Limitations of H.265 Codec Type:

- H.265 is not supported in MAXPRO Mobile app
- H.265 is not supported in Web client
- H.265 cameras utilizes CPU based Rendering

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 in a Primary/Redundant NVR 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 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.

Intended Audience

This guide is intended for the field and commissioning engineers of MAXPRO VMS system.

Structure of this Guide

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

No	Chapter	Description
1	<i>Commissioning Plan</i>	Description of the process involved in commissioning the MAXPRO VMS.
2	<i>Setting up the Client and the Server Computers</i>	Hardware specifications for MAXPRO VMS server and client computers. Procedures for configuring the monitor display properties. Steps for installing the serial expander.
3	<i>Installing the MAXPRO VMS R670 Software</i>	Procedure for installing MAXPRO VMS R670 software.
4	<i>Configuring devices and Setting up a Site</i>	Configure the MAXPRO VMS.
5	<i>Verifying the Configuration of MAXPRO VMS</i>	Steps to verify the configuration of MAXPRO VMS.
6	<i>Upgrade MAXPRO VMS</i>	Procedures to upgrade from previous versions for MAXPRO VMS to latest version of MAXPRO VMS.
7	<i>MAXPRO VMS Web Client</i>	Introduces Web client and describes procedure on how to install and use.

Typographical Conventions

This guide uses the conventions listed in the following table:

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

COMMISSIONING PLAN

Overview

Commissioning is the process of installing, configuring, and setting up the MAXPRO VMS hardware and software. At the end of the commissioning process, the MAXPRO VMS system is equipped for use by operators to perform surveillance operations. The steps in the commissioning process must be performed one after the other for successful deployment of MAXPRO VMS system.

Steps in the Commissioning Process

The process of commissioning consists of the following phases:

- *Setting up the Server and Client Computers.*
- *Installing the MAXPRO VMS R670 Software.*
- *Securing MAXPRO VMS*
- *Configuring the MAXPRO VMS System.*
- *Verifying the Configuration.*

Setting up the Server and Client Computers

Setting up the server and client computers involve:

- Determining the number of server and client computers at the location and ensuring that they meet the minimum hardware requirements such as processor type and memory size.
- to the computers after ensuring that they meet the hardware requirements. You can connect up to four monitors to each computer. After, configure the monitor display properties.

- Installing the serial expander, if switchers, serial keyboards (Ultrakey), Protocol Interface Translators (PIT), and other serial devices are used at the location.

Note: See the chapter [Setting up the Client and the Server Computers](#) for information on hardware requirements, how to connect the monitors to the computers, how to configure the display properties, and how to install the serial expander.

Installing the MAXPRO VMS R670 Software

Installing the software in the Server and Client Computers involves:

- Ensuring that the server and client computers meet the minimum software requirements such as operating system and anti virus software.
- Installing the MAXPRO VMS R670 software.

Caution: Don't install any Email client on the MAXPRO VMS Server machine.

Note: See the chapter [Installing the MAXPRO VMS R670 Software](#) for information on software requirements and installation instructions for the MAXPRO VMS R670 software.

Securing MAXPRO VMS

In this phase user is required to Logon to MAXPRO VMS application and secure it. Honeywell recommends you to change the default Password before you logon to MAXPRO VMS. Refer to MAXPRO VMS R670 Operators Guide and MAXPRO VMS Security Manual for further details. Follow the password requirements and password expiry policy accordingly as explained below.

Note: Old password is blank for Fresh installations.
In upgrade scenarios, enter the old password which is configured before upgrading.
Refer to MAXPRO VMS Security Manual for further details.

Password requirements

The following list highlights the password requirements:

- The password should have a minimum length of 12 characters.
- The password should consist of at least one number, one uppercase letter and one special character.

Note: It is recommended that previous 2 passwords should not match with new password.

Password Expiry

- For every user, password expires in 90 days. To recreate a new password, user needs to access Change Password feature in the login screen. Refer to MAXPRO VMS R670 Installation and Configuration Guide for more information.

- For specific users to disable the Password Expiry settings, navigate to Configurator > User tab and then select the Password Never Expires check box and then Save.

Note: It is recommended not to select the Password Never Expires check box for security norms.

Note: In Upgrade scenarios user will be able to login with same credentials but the password will expiry in 90 days. User needs to use the Change Password window in login screen for that particular user. For other users, logon to VMS application and change the password for all users in User's tab.

Configuring the MAXPRO VMS System

In this phase, you need to configure the MAXPRO VMS through the user interface. Before you start configuring, perform the following:

- Determine the number of sites to add in the MAXPRO VMS system. A default site is available in MAXPRO VMS. Typically, a site is a geographical group of cameras or similar cameras and can be used to logically group cameras.
- Determine the number of partitions and event groups to be created for each site. A default global partition is automatically created when you add a site in MAXPRO VMS. Partitions and event groups are used to limit access to cameras and events.
- Ensure that the recorders and other video devices such as cameras and streamers are powered on and connected to the network.

- Determine the IP addresses of the recorders and streamers. The IP addresses are required to add the devices to the MAXPRO VMS system.
- Determine to which site each recorder, camera, monitor, and switcher needs to be associated.
- Determine to which event group and partition each recorder, camera, switcher, and monitor needs to be associated.
- Determine the roles of users for each site. You need to create roles and define privileges for them while configuring the MAXPRO VMS system.
- Determine the number of users for each site. You need to create users and associate them to roles while configuring the MAXPRO VMS system. MAXPRO can also use Windows System users discoverable through Active directory
- Determine which partitions, event groups, client workstations, and joystick controllers (Ultrakey keyboard) each user can access.

Note: See the chapter [Configuring devices and Setting up a Site](#) for information on how to configure the MAXPRO VMS system.

Verifying the Configuration

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

Note: See the chapter [Verifying the Configuration of MAXPRO VMS](#) for information on how to perform the verification.

SETTING UP THE CLIENT AND THE SERVER COMPUTERS

Overview

This chapter explains about the setting the client and server computer for MAX-PRO VMS. Setting up the 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
- Hardware configuration of the computers
- Number of serial devices such as joystick controllers (Ultrakey keyboard), switchers, PITs, and other devices

Tasks to perform in this phase

The following table lists the activities that are performed in this phase.

Tasks	See the section...
Specifications for virtual server solution	Virtual Machine Specifications
Ensure that the hardware configuration of the server and client computers meet the minimum specifications.	Hardware Specifications
Connect the monitors, keyboard, and mouse to the server and client computers.	Configuring the Monitor Display Properties
Configure the monitor display properties.	Configuring the Monitor Display Properties.
Install the serial expander in the server to connect serial devices.	About Serial Expander

Virtual Machine Specifications

If you choose to provide your own virtual server solution for use with Honeywell MAXPRO VMS R670 VMS software, the solution must meet or exceed the specifications listed in the following table.

Specification	Description
Minimum Processors	Speed 3GHz, Sockets 2, Cores per socket 2 (2-vcpus)
Memory	16 GB
Storage	Two separate Disk/LUN datastores on a local SCSI, Fibre Channel or iSCSI Provisioned Thick "Eager-zeroed" preferred. Dedicated Datastore 1 sized 120GB or larger is for the Windows operating system, MAXPRO VMS server software and Microsoft SQL server software. Dedicated Datastore 2 sized 120GB or larger is for the Microsoft SQL Server database files
Networking	One or more active VM Network adapters 1000Mb, Full Duplex (vmxnet 3 preferred)
Video Card	Virtual Machine Video Card set to one display with 256MB total video memory
Operating System	For the VMware session install Windows Server 2012, 2016, 2019 Standard Edition 64 Bit

Note: You are responsible for the setup of the VMware ESXi host, the Virtual Machine configuration options, operating system software, physical and virtual networking configuration and all other customer IT requirements. Microsoft Windows Server 2012 or 2016 or 2019 64 Bit Standard Edition must be installed per the Honeywell installation instructions included on the MAXPRO VMS installation DVDs. Refer 800-15305V4_MAXPRO NVR and VMS VMware ESXi_Spec Notes for more information.

Caution: You own the full responsibility for the virtual solution, computer hardware and operating system compatibility. Honeywell is only responsible for the MAXPRO VMS software application and Honeywell-installed subsystem components. VMware ESXi qualification is for the MAXPRO VMS server only. The MAXPRO VMS client is not supported in a virtual environment.

Useful Tips

Here are some of the tips that help in setting up the virtual machine environment.

- MAXPRO VMS includes SQL Server 2019 Express (based on prerequisites) as default and supports SQL Server 2019
- The end customer has to provide, install, and maintain updates to Windows Defender 4.18.2101.9 Antivirus Software.
- Turn off the Microsoft automatic updates option.
- Always perform a full system backup prior to applying any of the tested Microsoft hot fixes.

- Follow the VMware ESXi best practices for configuring ESXi hosts and minimize SCSI Reservation delays. To support 64-bit virtual machines, support for hardware virtualization (Intel VT-x) must be enabled on x64 CPUs on the Physical ESXi Host Server. Place the management network and virtual machine networks on different physical network cards. Dedicated Gigabit Ethernet cards for virtual machines, such as Intel PRO 1000 adapters, improve throughput to virtual machines with high network traffic.

Hardware Specifications

The MAXPRO VMS server and client computers must meet the minimum hardware specifications. This is necessary for proper and efficient working of the MAXPRO VMS.

There are two types of hardware configurations for the server and client namely, standard and performance. The standard configuration uses the minimum hardware specifications. The performance configuration uses higher hardware specifications for better performance. The performance configuration is also recommended for compatibility with features that are going to be provided in MAXPRO VMS in the near future.

Note: *32 bit systems are not supported.*

MAXPRO VMS Server (Performance Spec with Windows 2012 Server Standard R2 64 bit, Windows 2016 Server Standard 64 bit, Windows 2019 Server Standard 64 bit up to 10 Clients)

Specification	Description
Processor	Intel Quad Core Xeon E3 1225V3 3.2GHz S1150
Recommended Operating System	Microsoft Windows® 2012 Server STD 64 Bit (Only for Upgrade) Microsoft Windows® 2016 Server STD 64 Bit (Recommended for Fresh Installation) Microsoft Windows® 2019 Server STD 64 Bit (Recommended for Fresh Installation)
Recommended Computer Type (Server or Workstation)	Server - dual power supply suggested
Recommended System Memory (RAM)	16GB
DVD Drive (RW (Read Write) is required if workstation is used for exporting recordings)	DVD +/- RW
Disk	Two separate hard drives or two sets of RAID arrays Disk / RAID set 1 utilizes 10K RPM SATA 150GB or 10K-15K RPM SCSI 146GB for Windows operating system, MAXPRO VMS Server Software, Microsoft SQL Server software Disk / RAID set 2 utilizes 10K RPM SATA 150GB or 10K-15K RPM SCSI 146GB for MAXPRO VMS database files Microsoft SQL Server database files Note: if fault tolerance is required RAID set one is RAID 1, 10 or 0+1 and RAID set two is RAID 10 or 0 + 1.
Multiple Monitor Card -Display Adapter (Video Resolution)	Display Adapter with Video resolution 1024x768 pixels; 32-bit color or higher
Serial Ports	Only required if serial device are to be connected - Suggested 8 Port MOXA PCI-e serial RS232
Network Connection	1Gbit/sec or greater.

MAXPRO VMS Server (Performance Spec with Windows 2012 Server Standard R2 64 bit, Windows 2016 Server Standard 64 bit, Windows 2019 Server Standard 64 bit up to 25 Clients)

Specification	Description
Processor	Intel 6 Core Xeon E5 2630V2 2.6GHz S2011
Recommended Operating System	Microsoft Windows® 2012 Server STD 64 Bit (Only for Upgrade) Microsoft Windows® 2016 Server STD 64 Bit (Recommended for Fresh Installation) Microsoft Windows® 2019 Server STD 64 Bit (Recommended for Fresh Installation)
Recommended Computer Type (Server or Workstation)	Server - dual power supply suggested
Recommended System Memory (RAM)	32 GB (add “/pae” to boot.ini file to recognize more than 4GB of RAM)
DVD Drive (RW (Read Write) is required if workstation is used for exporting recordings)	DVD +/- RW
Disk	Two separate hard drives or two sets of RAID arrays Disk / RAID set 1 utilizes 10K RPM SATA 150GB or 10K-15K RPM SCSI 146GB for Windows operating system, MAXPRO VMS Server Software, Microsoft SQL Server software Disk / RAID set 2 utilizes 10K RPM SATA 150GB or 10K-15K RPM SCSI 146GB for MAXPRO VMS database files Microsoft SQL Server database files Note: if fault tolerance is required RAID set one is RAID 1, 10 or 0+1 and RAID set two is RAID 10 or 0 + 1.
Multiple Monitor Card - Display Adapter (Video Resolution)	Display Adapter with Video resolution 1024x768 pixels; 32-bit color or higher
Serial Ports	Only required if serial device are to be connected - Suggested 8 Port MOXA PCI-e serial RS232
Network Connection	1Gbit/sec or greater.

MAXPRO VMS Server (Performance Spec with Windows 2012 Server Standard R2 64 bit, Windows 2016 Server Standard 64 bit, Windows 2019 Server Standard 64 bit above 25 Clients)

Specification	Description
Processor	Intel two Quad Core Xeon E5 2630V2 2.6GHz S2011
Recommended Operating System	Microsoft Windows® 2012 Server STD 64 Bit (Only for Upgrade) Microsoft Windows® 2016 Server STD 64 Bit (Recommended for Fresh Installation) Microsoft Windows® 2019 Server STD 64 Bit (Recommended for Fresh Installation)
Recommended SQL	Full version of SQL for 2014/2016/2017. For Fresh installation, if the machine does not have the latest version of SQL then the installer will install SQL 2019 Express version. For Upgrade scenario, the system will retain the previously installed SQL version.
Recommended Computer Type (Server or Workstation)	Server - dual power supply suggested
Recommended System Memory (RAM)	32 GB (add "/pae" to boot.ini file to recognize more than 4GB of RAM)
DVD Drive (RW (Read Write) is required if workstation is used for exporting recordings)	DVD +/- RW
Disk	Two separate hard drives or two sets of RAID arrays Disk / RAID set 1 utilizes 10K RPM SATA 150GB or 10K-15K RPM SCSI 146GB for Windows operating system, MAXPRO VMS Server Software, Microsoft SQL Server software Disk / RAID set 2 utilizes 10K RPM SATA 150GB or 10K-15K RPM SCSI 146GB for MAXPRO VMS database files Microsoft SQL Server database files Note: if fault tolerance is required RAID set one is RAID 1, 10 or 0+1 and RAID set two is RAID 10 or 0 + 1.
Multiple Monitor Card - Display Adapter (Video Resolution)	Display Adapter with Video resolution 1024x768 pixels; 32-bit color or higher
Serial Ports	Only required if serial device are to be connected - Suggested 8 Port MOXA PCI-e serial RS232
Network Connection	1Gbit/sec or greater.

MAXPRO VMS Workstation Computer (Standard Spec with Windows 10 Enterprise 64-Bit (Upgrade Only) up to 1 monitors)

Specification	Description
Processor	Intel(R) Core(TM) i7-8700 CPU @ 3.4GHz
Recommended Operating System	Microsoft Windows® 10 Enterprise (64 bit)
Recommended Computer Type (Server or Workstation)	Workstation
Recommended System Memory (RAM)	8GB.
DVD Drive (RW (Read Write) is required if workstation is used for exporting recordings)	DVD +/- RW.
Disk	Single Disk or RAID 0 or 0+1 10K SATA 80GB or 10K to 15K SAS 73GB: Windows Operating System
Multiple Monitor Card - Display Adapter (Video Resolution)	1 x 1024 MBPCIe x16 NVIDIA NVS510, DVI or VGA or HDMI Intel® HD Graphics Version 25.20.100.6617
Network Connection	1Gbit/sec or greater.
Video Resolution	1920*1080P and 4k

MAXPRO VMS Workstation Computer (Standard Spec with Windows 10 Enterprise 64-Bit (Upgrade Only) up to 2 monitors)

Specification	Description
Processor	Intel(R) Core(TM) i7-8700 CPU @ 3.4GHz
Recommended Operating System	Microsoft Windows® 10 Enterprise (64 bit)
Recommended Computer Type (Server or Workstation)	Workstation
Recommended System Memory (RAM)	8GB.
DVD Drive (RW (Read Write) is required if workstation is used for exporting recordings)	DVD +/- RW.

Specification	Description
Disk	Single Disk or RAID 0 or 0+1 10K SATA 80GB or 10K to 15K SAS 73GB: Windows Operating System
Multiple Monitor Card - Display Adapter (Video Resolution)	2 x 1990MB PCIe x16 NVIDIA NVS 300, Dual DVI or Dual VGA or DVI+VGA. This is for a four monitor setup with each monitor requiring 1024 MB approximately Intel® HD Graphics Version 25.20.100.6617
Network Connection	1Gbit/sec or greater
Video Resolution	1920*1080P and 4k

MAXPRO VMS Workstation Computer (Standard Spec with Windows 10 Enterprise 64-Bit (Upgrade Only) up to 4 monitors)

Specification	Description
Processor	Intel(R) Core(TM) i7-8700 CPU @ 3.4GHz
Recommended Operating System	Microsoft Windows® 10 Enterprise (64 bit)
Recommended Computer Type (Server or Workstation)	Workstation
Recommended System Memory (RAM)	16GB.
DVD Drive (RW (Read Write) is required if workstation is used for exporting recordings)	DVD +/- RW.
Disk	Single Disk or RAID 0 or 0+1 10K SATA 80GB or 10K to 15K SAS 73GB: Windows Operating System
Multiple Monitor Card - Display Adapter (Video Resolution)	4 x 4038 MB PCIe x16 NVIDIA NVS 510, Dual DVI or Dual VGA or DVI+VGA. This is for a four monitor setup with each monitor requiring 1024 MB approximately. Intel® HD Graphics Version 25.20.100.6617
Network Connection	1Gbit/sec or greater
Video Resolution	1920*1080P and 4k

MAXPRO VMS Analytics Server Specification

Specification	Description
Processor	Intel® Core™ 2 Duo Processor E6750 2.66 GHz or Quad Core Intel® Xeon® Processor X5450 (3.00GHz,2X6M L2,1333)
Recommended Operating System	Microsoft Windows® 10 Enterprise (64 bit) Microsoft Windows® 2012 Server STD 64 Bit Microsoft Windows® 2016 Server STD 64 Bit Microsoft Windows® 2019 Server STD 64 Bit
Recommended Computer Type (Server or Workstation)	Workstation
Recommended System Memory (RAM)	16GB.
DVD Drive (RW (Read Write) is required if workstation is used for exporting recordings)	DVD +/- RW.
Disk	Single Disk or RAID 0 or 0+1 10K SATA 80GB or 10K to 15K SAS 73GB; Windows Operating System
Multiple Monitor Card - Display Adapter (Video Resolution)	NVIDIA NVS 510 – 1024 MB RAM
Network Connection	1Gbit/sec or greater
Video Resolution	1920*1080P and 4k

MAXPRO VMS Workstation Computer with Prowatch client (Performance Spec with Windows 8.1 Professional 64 Bit, supports up to 2 monitors)

Specification	Description
Processor	Quad Core Intel® Xeon® Processor E5620 (12M Cache, 2.40 GHz, 5.86 GT/s Intel® QPI).
Recommended Operating System	Microsoft Windows® 8.1 Professional 64 Bit Few of the recorders run only on specific operating systems. Before installing the device drivers for the recorders, please refer to the “Operating Systems” sheet in the MAXPROVMS_HW_SW_Compatibility_Matrix.xls file available on the MAXPRO VMS R550 DVD.
Recommended Computer Type (Server or Workstation)	Workstation.

Specification	Description
Recommended System Memory (RAM)	8 GB.
DVD Drive (RW (Read Write) is required if workstation is used for exporting recordings)	DVD-RW drive.
Disk	Single Disk or RAID 0 or 0+1 10K SATA 80GB or 10K to 15K SAS 73GB: Windows Operating System.
Multiple Monitor Card - Display Adapter (Video Resolution)	1 x 256MB PCIe x16 NVIDIA Quadro NVS 285, Dual DVI or Dual VGA or DVI+VGA. This is for a two monitor setup with each monitor requiring 128 MB.
Network Connection	1Gbit/sec or greater.
Video Resolution	1024x768 pixels; 24 bit color or higher.

Configuring the Monitor Display Properties

The recommended display settings for the monitor are page resolution of 1024 x 768 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.

To configure the display settings from the context menu in the Windows desktop

1. Right-click the Windows desktop to display the context-menu.
2. Click Properties. The Display Properties page appears.
3. Click the Settings tab.
4. Select the page resolution and color quality.
5. Click Apply to save the settings.
6. Click OK to close the page.

To configure the display settings from the Windows control panel

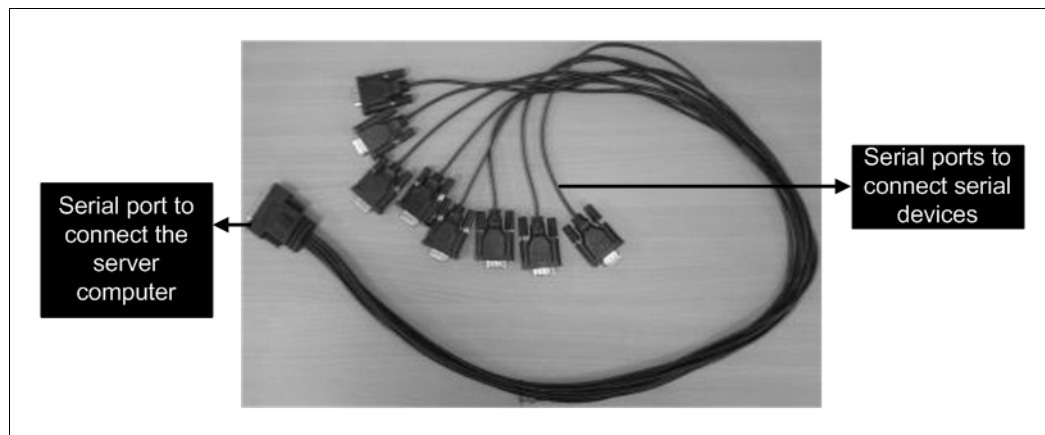
1. Go to Windows control panel.

Note: To open the control panel, click Start > Settings > Control Panel.

2. Double-click the Display icon. The Display Properties page appears.
3. Click the Settings tab.
4. Select the page resolution and color quality.
5. Click Apply to save the settings.
6. Click OK to close the page.

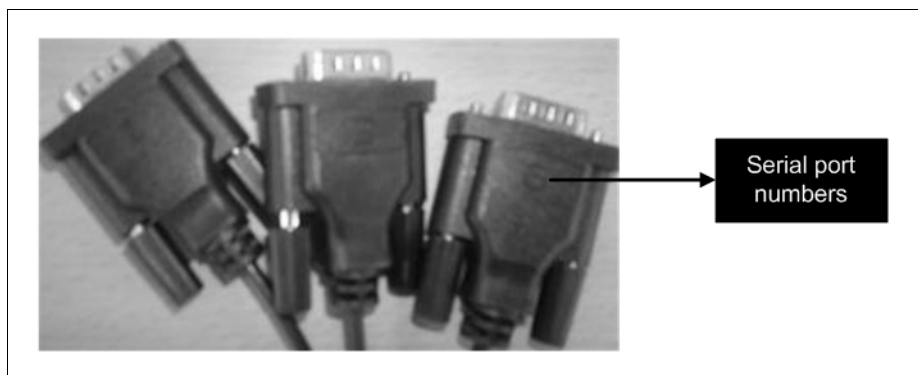
About Serial Expander

The serial expander cable is used for increasing the number of serial ports in the computer. One end of the serial expander cable connects to a serial port in the computer. The other end of the serial expander cable consists of eight serial ports to which you can connect serial devices. For example, you can install the serial expander in the server to connect serial devices such as switchers, joystick controllers (Ultrak keyboard), and PITs used at the location. The following figure illustrates a serial expander cable.



Each of the eight serial ports in the serial expander cable is marked with a number. This number is used for identifying the serial port while configuring the settings such as baud rate, data bits, and others using the MAXPRO VMS software.

The following figure illustrates the serial port numbering in the serial expander cable.



Enabling Windows .NET 3.5

This section describes the procedure to enable .NET 3.5 on Windows 8 and Server 2012 machine with/without Internet connection.

Note: This section is not applicable for Windows 7 and Server 2008 machines to enable .NET 3.5.

To enable .NET 3.5 on Windows 8 machine using internet connection

1. Click Start > Control Panel > Programs and Features. The Programs and Features window appears.

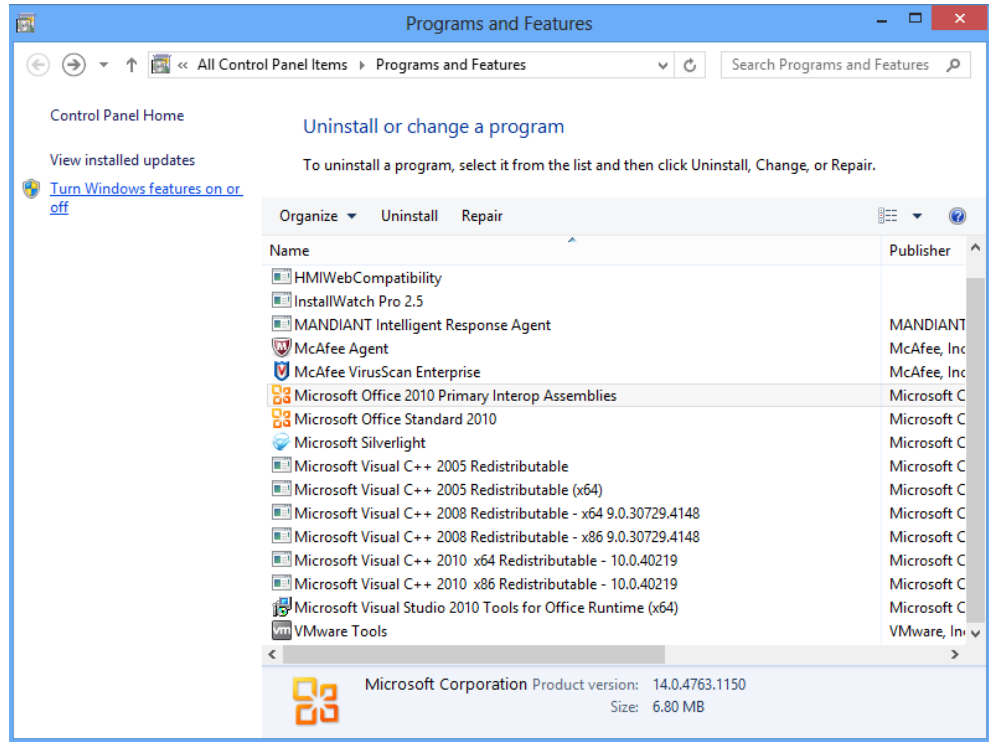


Figure 2-1 Program and Features

2. Under Control Panel Home pane, click Turn Windows features on or off link. The Windows Features page appears.

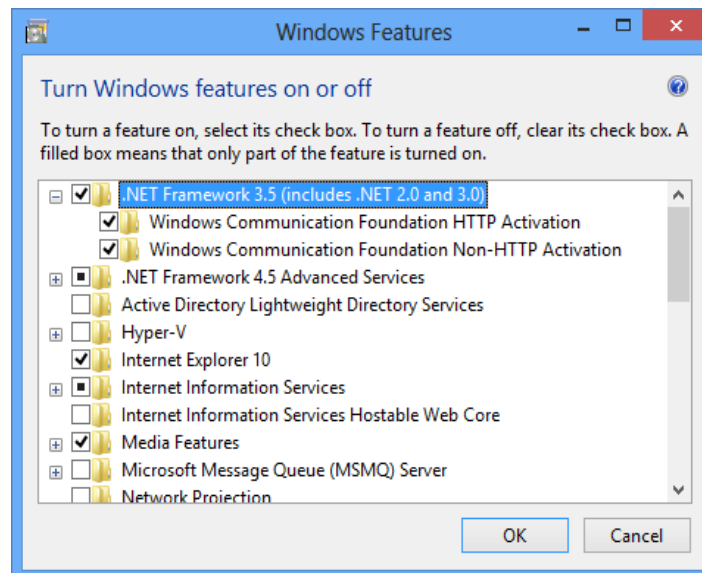


Figure 2-2 Windows Features

3. Select the following check boxes and then click OK.

- .Net Framework 3.5 (includes .Net2.0 and 3.0)
- Windows Communication Foundation HTTP Activation
- Windows Communication Foundation Non-HTTP Activation

To enable .NET 3.5 on Windows Server 2012 machine using internet connection

1. Navigate to Server Manager -> Manage and then click Add Roles and features link.
Or
Navigate to Server Manager -> Dashboard -> Configure this local server and then click Add Roles and features link as shown below.

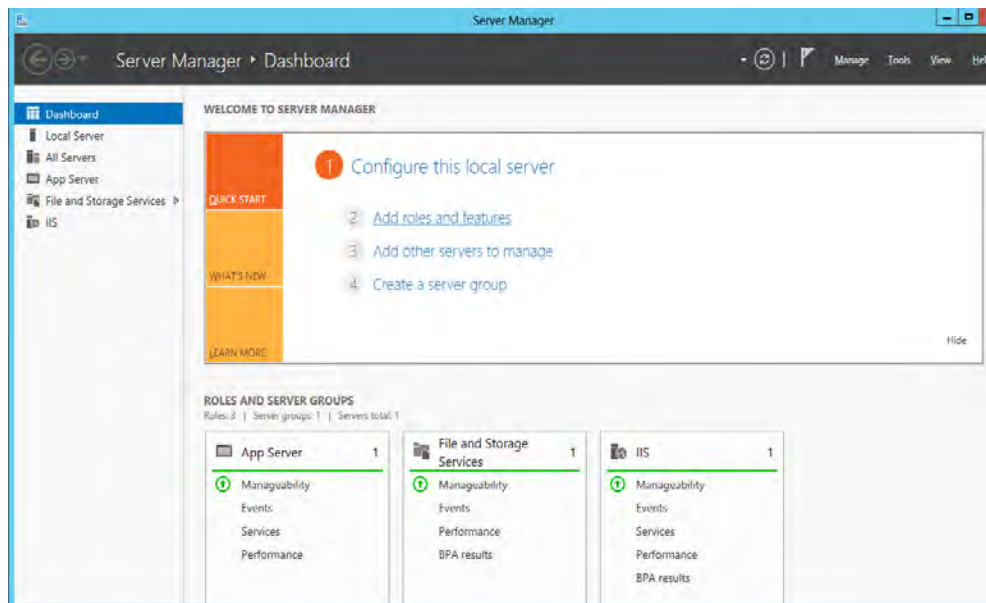


Figure 2-3 Server Manager Window

The Add Roles and Features Wizard appears.

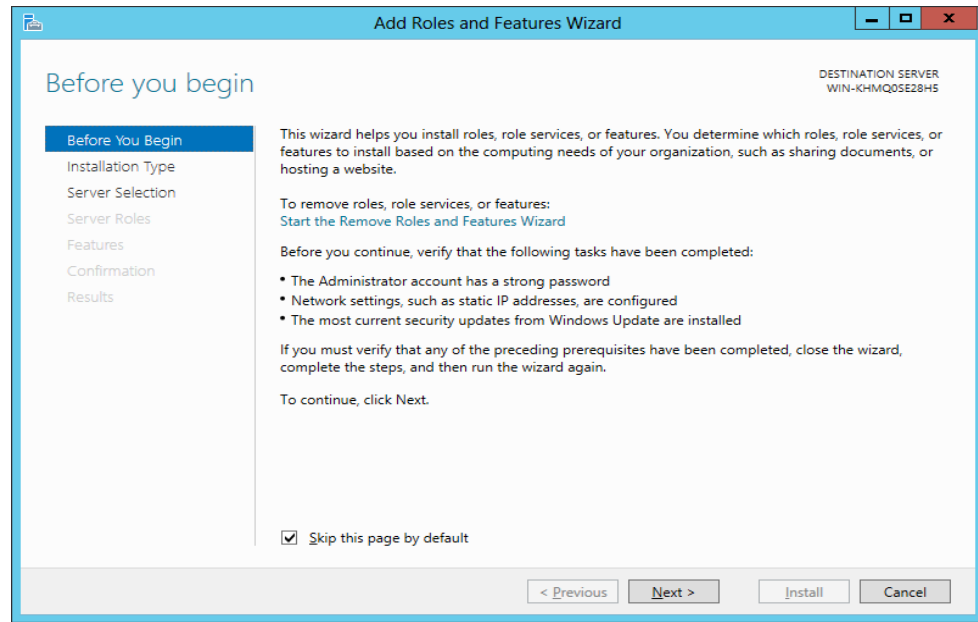


Figure 2-4 Add Roles and Features Wizard

2. Click Next. The Add Role and Features Wizard appears.

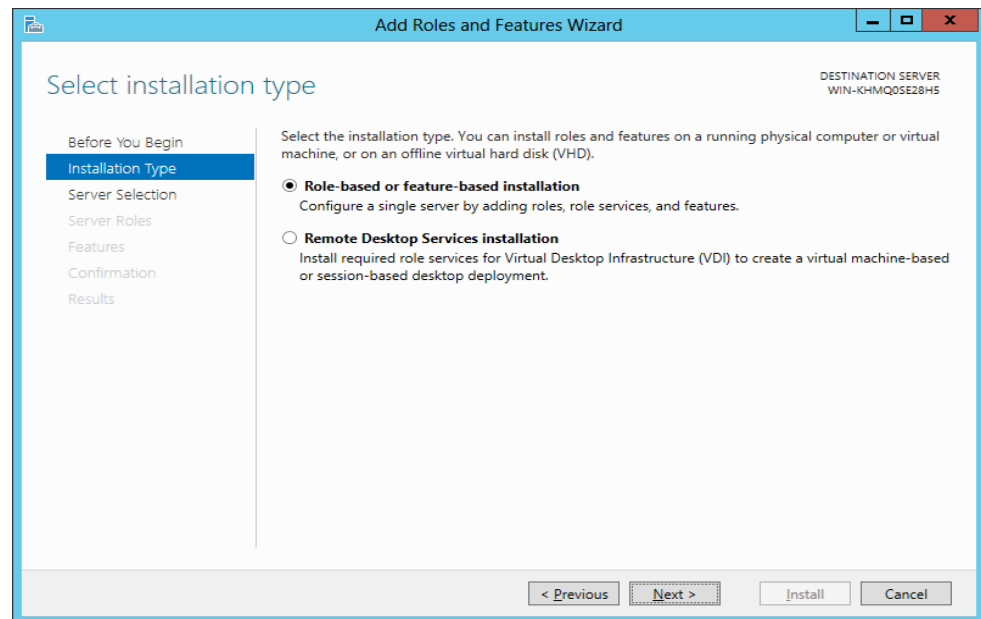


Figure 2-5 Select Installation type

3. Click Role-based or feature- based installation option and then click Next. The Select Destination Server screen appears.

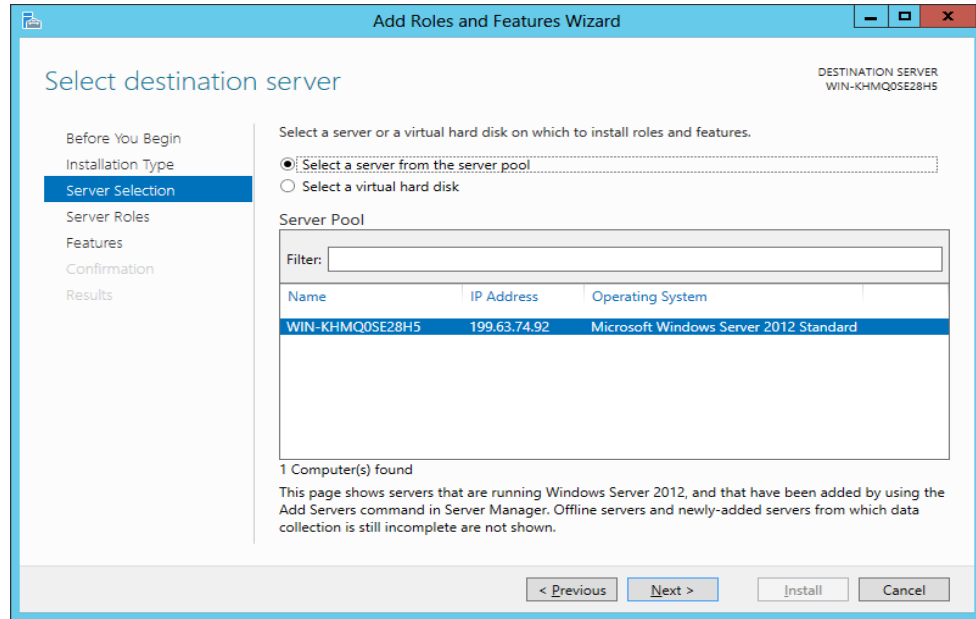


Figure 2-6 Select destination server

4. Click Select a server from the server pool option and then select the current machine name listed under Server Pool. Click Next. Select server roles screen appears.

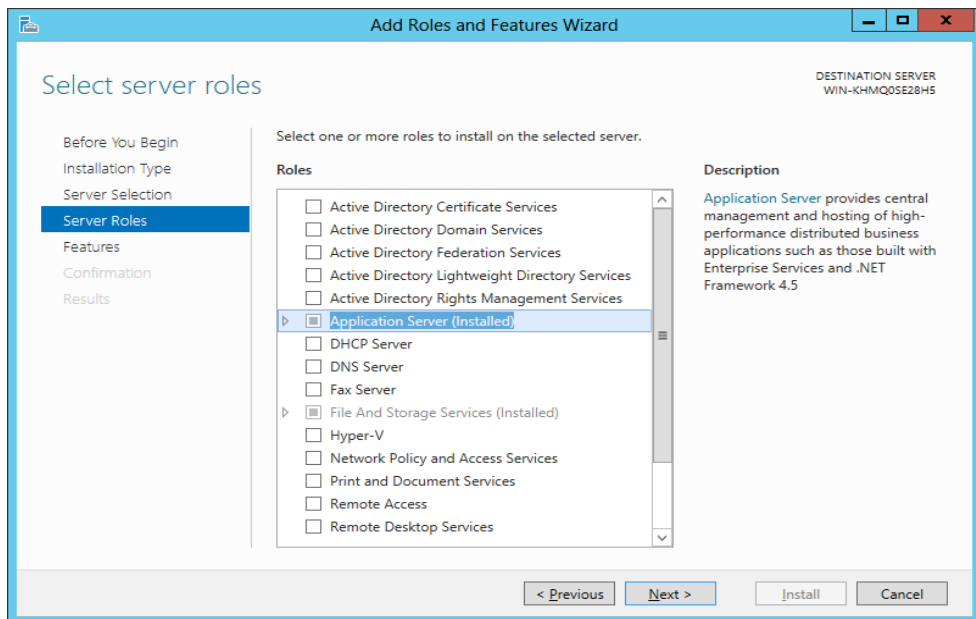


Figure 2-7 Select Server Roles

5. Under Roles, select the Application server (Installed) check box and then click Next. The Add Roles and Features Wizard appears

Note: The Add Roles and Features Wizard displayed differs on the HTTP Activation and Non-HTTP Activation features.

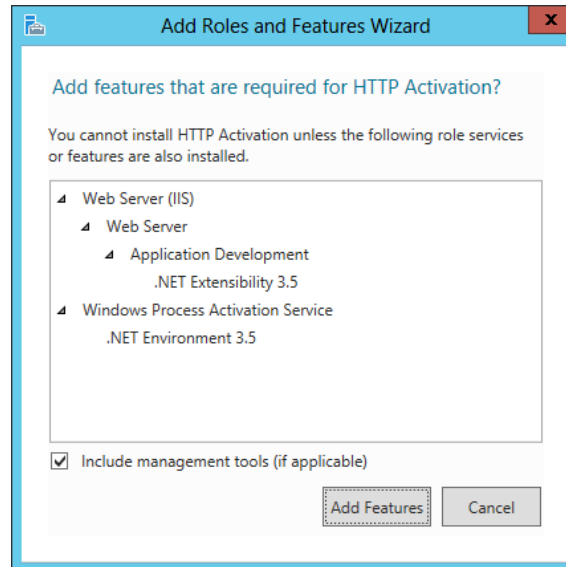


Figure 2-8 HTTP Activation

6. Click Add Features button.

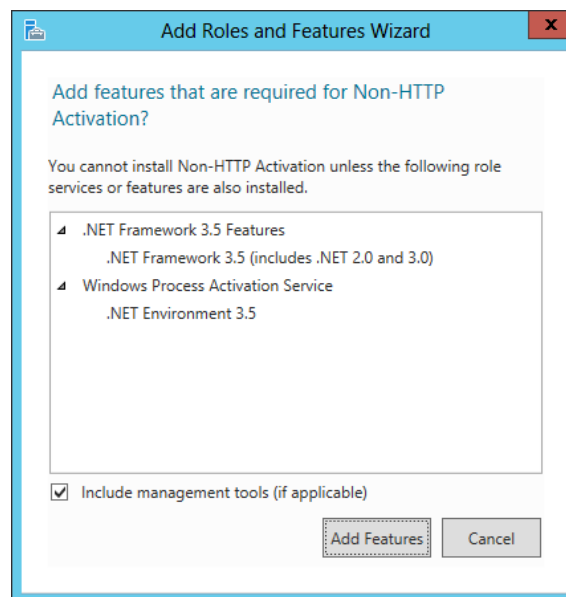


Figure 2-9 Non-HTTP Activation

7. Click Add Features. The Select Features screen appears.

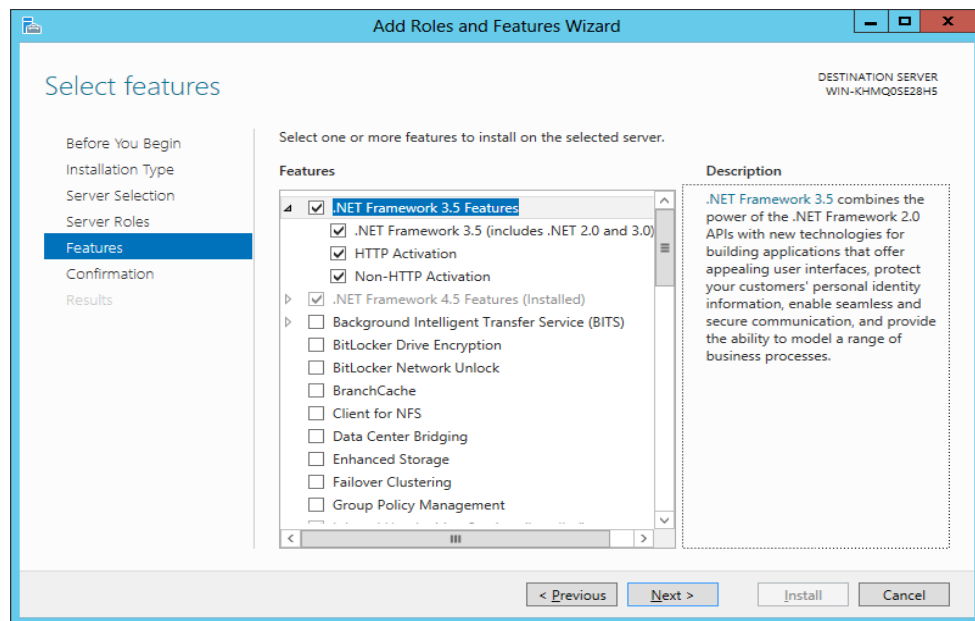


Figure 2-10 Select Features

8. Select the following feature check boxes in the Features pane:

- .Net Framework 3.5 features
- .Net Framework 3.5 (includes .Net 2.0 and 3.0)
- HTTP Activation
- Non-HTTP Activation

9. Click Next. The Confirm installation selection screen appears.

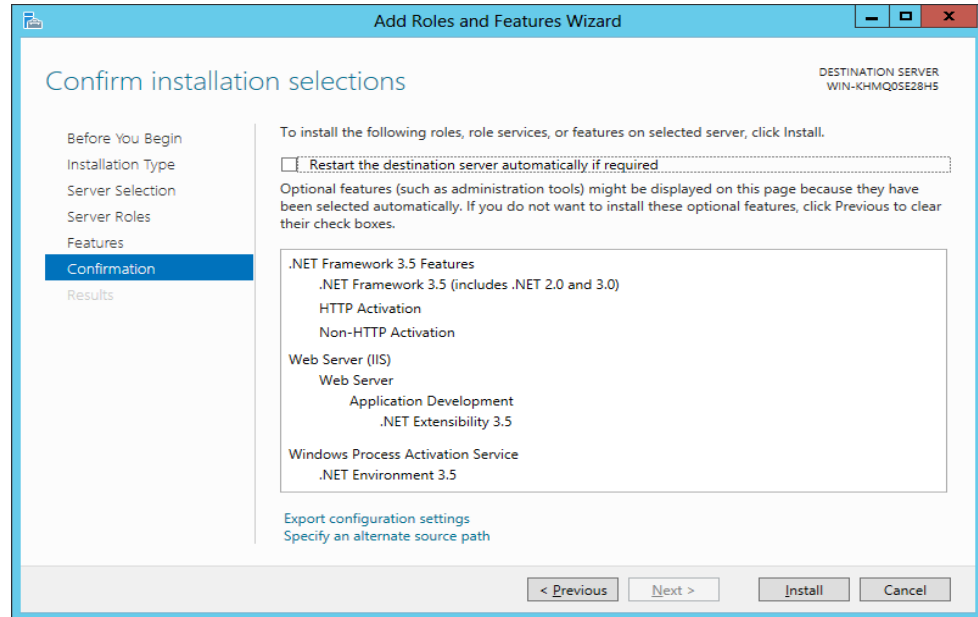


Figure 2-11 Confirm Installation Selection

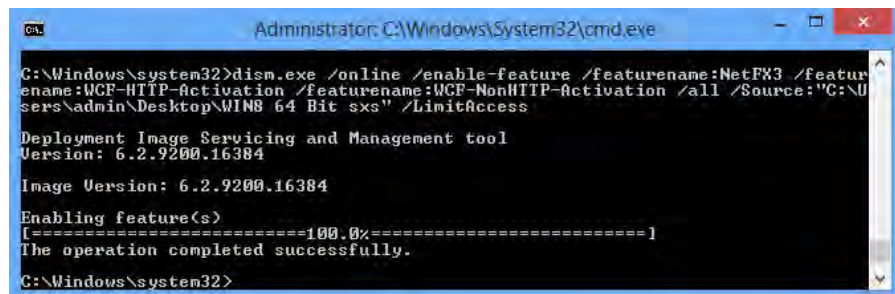
10. Click Install.

To enable .NET 3.5 on Windows 8 and Server 2012 machine without internet connection

1. Insert the Windows OS DVD in the DVD drive.
2. Browse the Sxs folder and copy the path. For Example: E:\Sources\Sxs.
3. Execute the following command from the command prompt window using the Administrative privileges. The <<PATH_TO_WIN_SXS_FOLDER>> should be replaced with the actual path of Sxs folder as explained in step 2.

```
%WINDIR%\system32\dism.exe /online /enable-feature /featurename:NetFX3 /featurename:WCF-HTTP-Activation /featurename:WCF-NonHTTP-Activation /all /Source:<<PATH_TO_WIN_SXS_FOLDER>> /LimitAccess
```

Note: Use the cmd.exe available in the path C:\windows\system32 folder on 64 bit Operating System.



NetBIOS Naming Convention Limitations

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

For MAXPRO NVR

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

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

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

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

This page is intentionally left blank

INSTALLING THE MAXPRO VMS R670 SOFTWARE

Overview

This chapter describes the procedures for installing MAXPRO VMS R670 software application. Follow the appropriate section in this chapter to complete the software installation.

- MAXPRO®VMS R670: See [How to Install MAXPRO™ VMS R670](#)

Before you begin

Ensure that:

1. the client and server computers meet the software requirements.
2. Windows Updates are disabled.
3. UAC is disabled.
4. you have configured the user credentials which never expires in Computer Management window.
5. Refer to the [MAXPRO VMS R650 Permissions and Recommendations Technical Notes](#) for SQL pre and post installation requisites.
6. User should have .Net 4.6.1 installed on Windows 10 and Windows 2012 OS machine.
7. Installed the SQL Service Pack on older SQL Server versions (any SQL version below 2016) to work with MAXPRO VMS. Refer to the [MAXPRO VMS-NVR Security Manual](#) for more information.

System Requirements

The client and server computers must meet the following specifications.

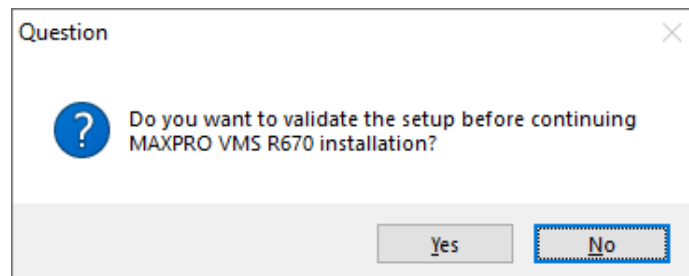
Specification	Description
Operating System	Server Installation: Windows 2016 and Windows 2019 (64 Bit Only) NVR Server Installation - Windows 2016, Windows 2019 and Windows 10 (64 Bit Only) Client Installations (VMS and NVR clients) - Windows 10 (64 Bit Only). Note: 32 bit systems are not supported.
SQL Version	If the machine does not have SQL then the installer will install SQL 2019 version. It also support full version of 2014/2016/2017 SQL
Antivirus	Windows Defender V 4.18.2101.9
Monitor Resolution	Minimum 1024x768 pixels, Up to 4K. For 4K monitor ensure High DIP setting as override option is enabled

How to Install MAXPRO™ VMS R670

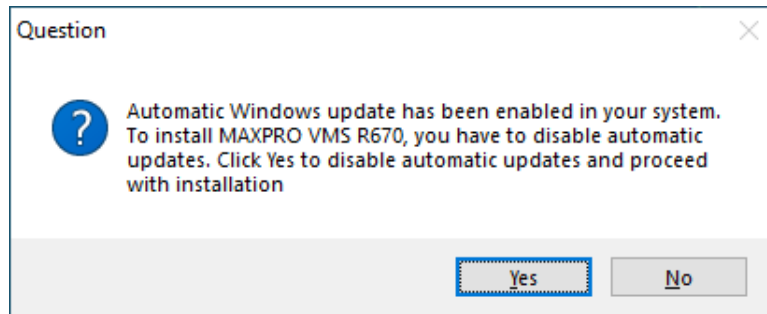
Note: The installing user should be administrator or domain/work group administrator

To install MAXPRO™ VMS R670

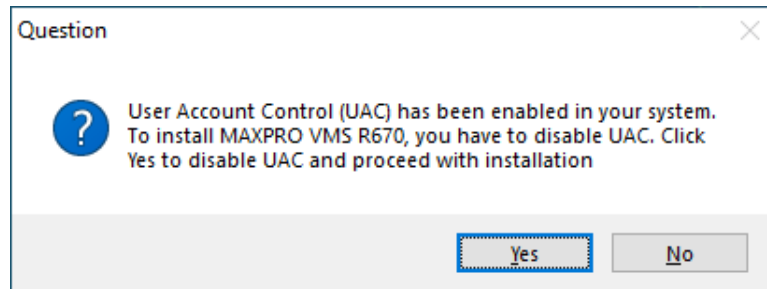
1. Insert the MAXPRO VMS R670 DVD in the DVD drive. The setup runs automatically. If the setup does not run automatically, browse to the setup folder on the DVD and double-click Setup.exe. A validation message is displayed as shown below.

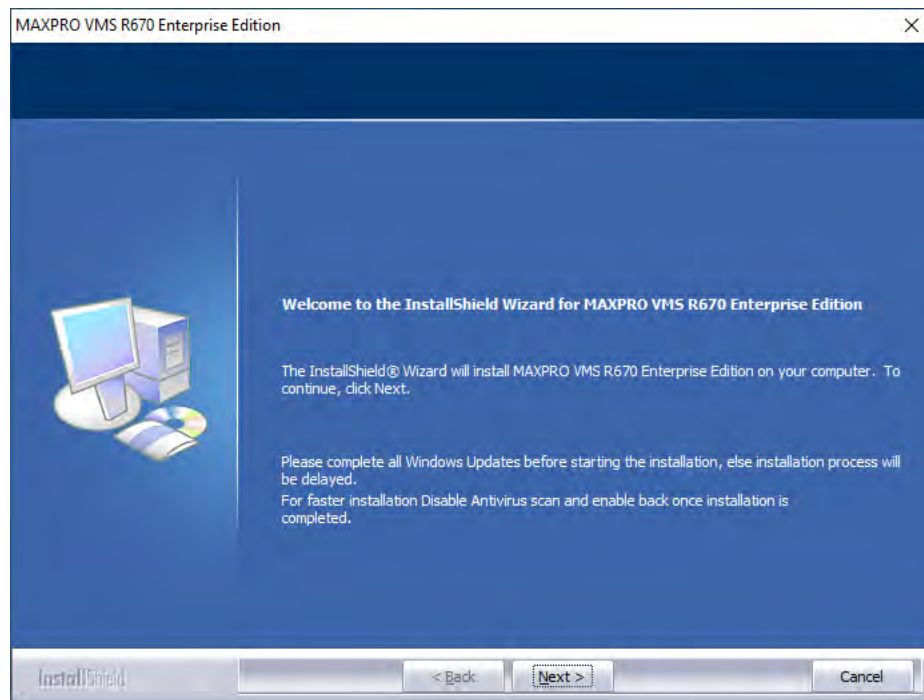


2. Click Yes to validate. The following messages are displayed.
 - A message if there are any pending reboots due to latest Windows updates is displayed. Click **OK** to perform a reboot and then continue with installation.
 - A confirmation message is displayed to disable the Automatic Windows updates as shown below. Click **Yes** to disable and proceed.

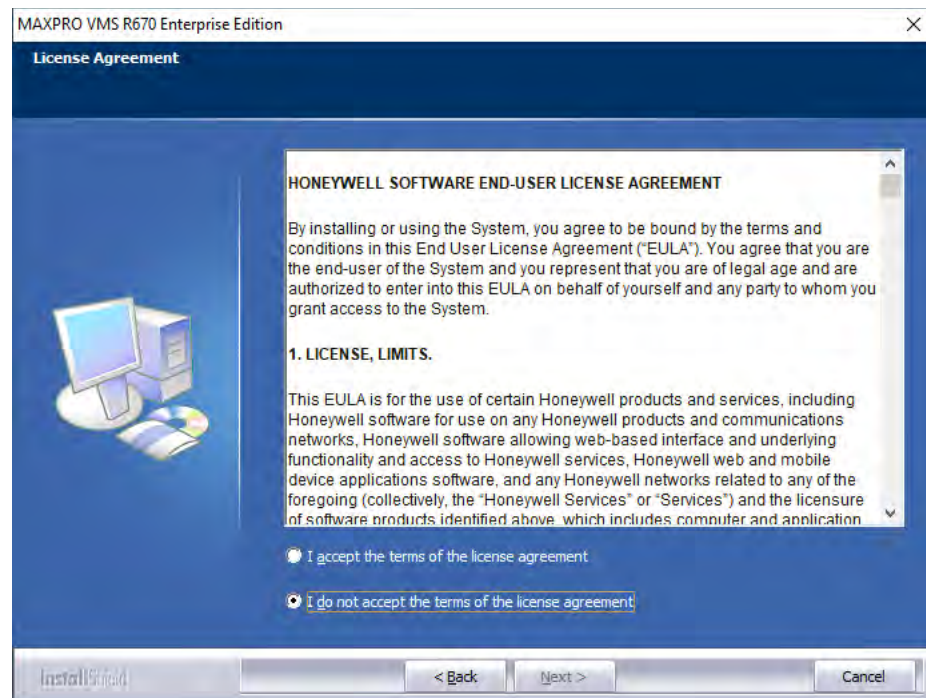


- A confirmation message is displayed to disable the User Account Control as shown below. Click **Yes** to disable and proceed. The Install Shield Wizard displays the **Welcome** page.

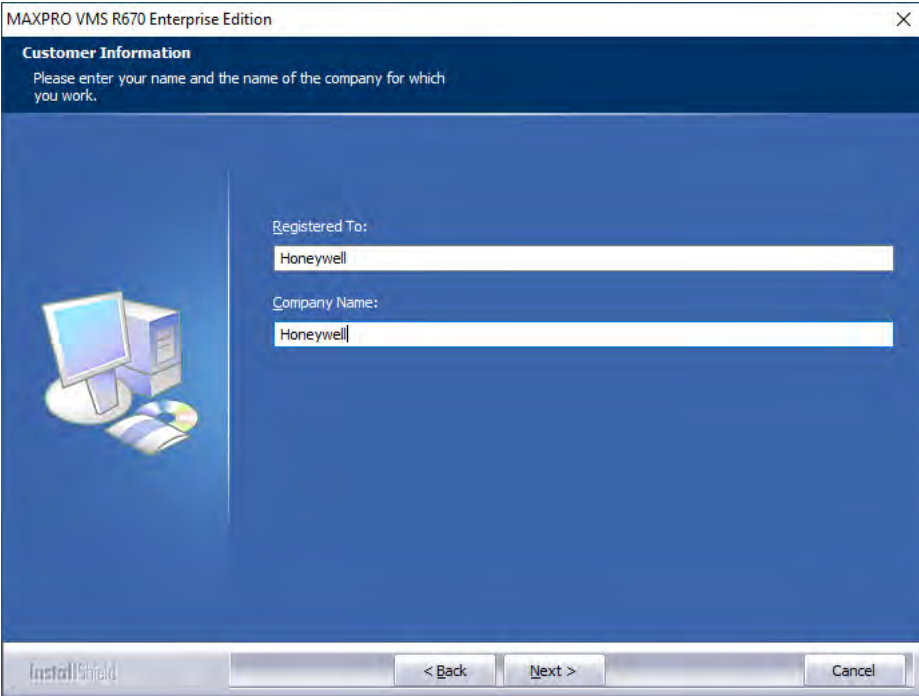




3. Click Next. The License Agreement page appears. This page displays the license agreement details for the MAXPRO VMS software.

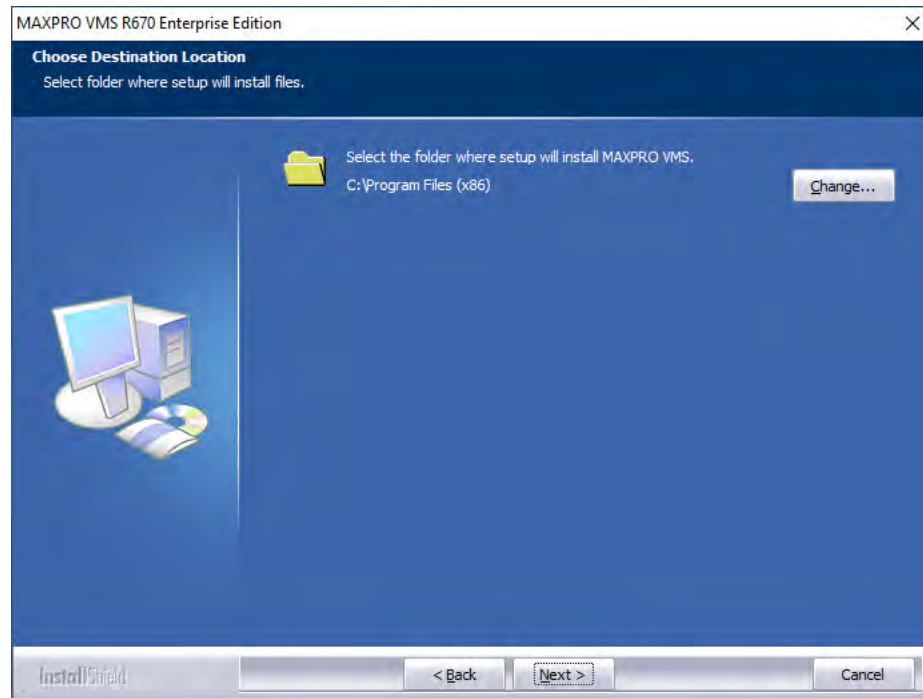


4. Read the license agreement, and then click I accept the terms of the license agreement to accept the license agreement.
5. Click Next. The Customer Information page appears.



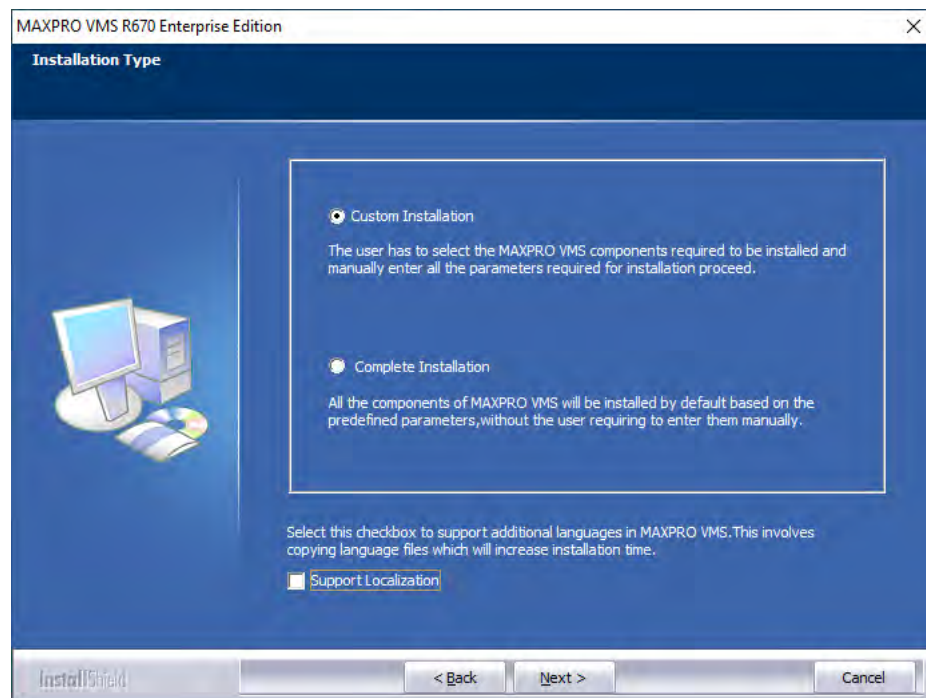
The image shows a Windows-style dialog box titled "MAXPRO VMS R670 Enterprise Edition". The dialog has a dark blue header bar with the title and a close button (X). Below the header, the text "Customer Information" is displayed, followed by the instruction "Please enter your name and the name of the company for which you work." The main area of the dialog is light blue and contains two text input fields. The first field is labeled "Registered To:" and contains the text "Honeywell". The second field is labeled "Company Name:" and also contains the text "Honeywell". To the left of the input fields is a small graphic of a computer monitor, a tower unit, and a CD/DVD. At the bottom of the dialog, there is a silver bar containing the "InstallShield" logo on the left and three buttons: "< Back", "Next >", and "Cancel".

6. In the Registered To box, type your name.
7. In the Company Name box, type your company name.
8. Click Next. The Choose Destination Location dialog box appears.



Note: Honeywell recommends you to install the MAXPRO VMS R670 software in C drive. By default C drive is selected. Click Change to change the default destination folder, and then select the path to install.

9. Click Next. The Installation Type page appears.



10. Select Custom Installation or Complete Installation as applicable. Use the instructions in one of the following sections that corresponds to the feature that you are installing, [Complete Installation](#) or [Custom Installation](#)
11. Select the Support Localization check box to support additional languages in MAXPRO VMS. By default this check boxes is not selected.

Note: This involves copying language files and it may increase the installation time.

Complete Installation	Installs MAXPRO VMS Server, MAXPRO VMS Client, MAXPRO VMS Scheduler, MAXPRO VMS Trinity Framework, Device drivers, Adapters and Analytics Sever and Client. See Complete Installation .
Custom Installation	Helps you to choose between MAXPRO VMS Server, MAXPRO VMS Client and Analytics Sever and Client. See Custom Installation . Choosing the "Custom Installation" option can save the installation time by eliminating the installation of any unnecessary modules.

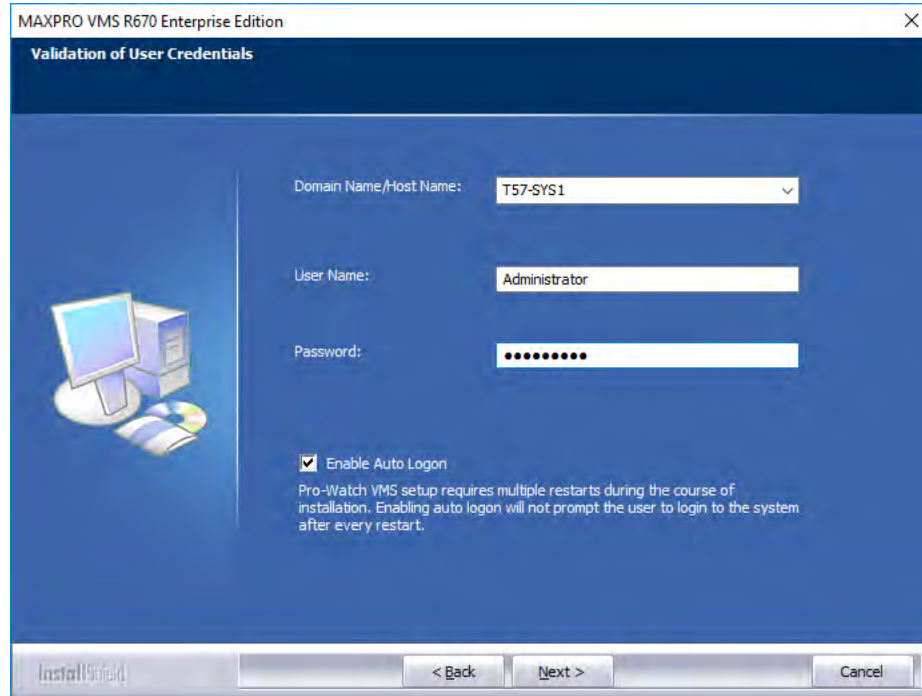
Complete Installation

Before you begin

Complete installation includes:

- Server and Client
- Install Video Analytics Server

1. Perform step 1 through step 9 of [How to Install MAXPRO™ VMS R670](#), select Complete Installation in the Installation Type page.
2. Click Next. The Validation of User Credentials appears.

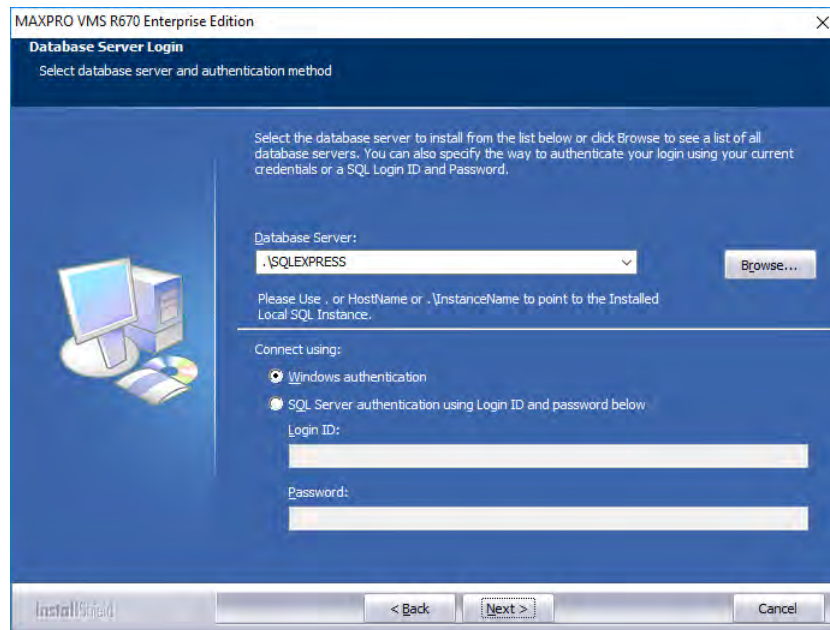


3. Select your Domain Name/Host Name.
4. Type your Windows User Name.
5. Type your Windows Password.

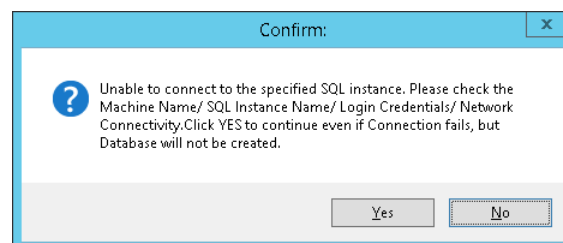
Note: Honeywell recommends to use the newly created Administrator user account as explained in *Securing MAXPRO VMS and NVR Guide*.

6. Click Next. The confirmation message is displayed to enable Auto Logon. Click Yes. The Database Server Login window appears.

Note: Select Standard or Enterprise version of SQL to install R670.

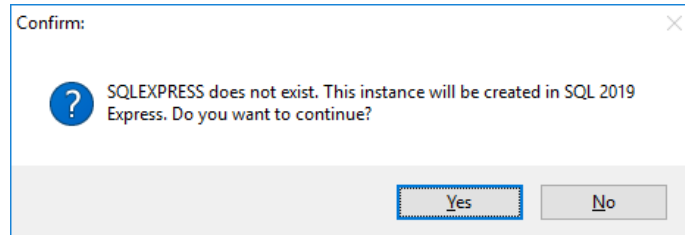


7. Click Browse, and then select any existing SQL database. You can select the existing SQL database on the same network or from a remote computer. If you do not want to select an existing database, proceed to step 9. If SQL instance exists and not in running state then an error message is displayed as shown below. User need to manually start the SQL service in services console window.

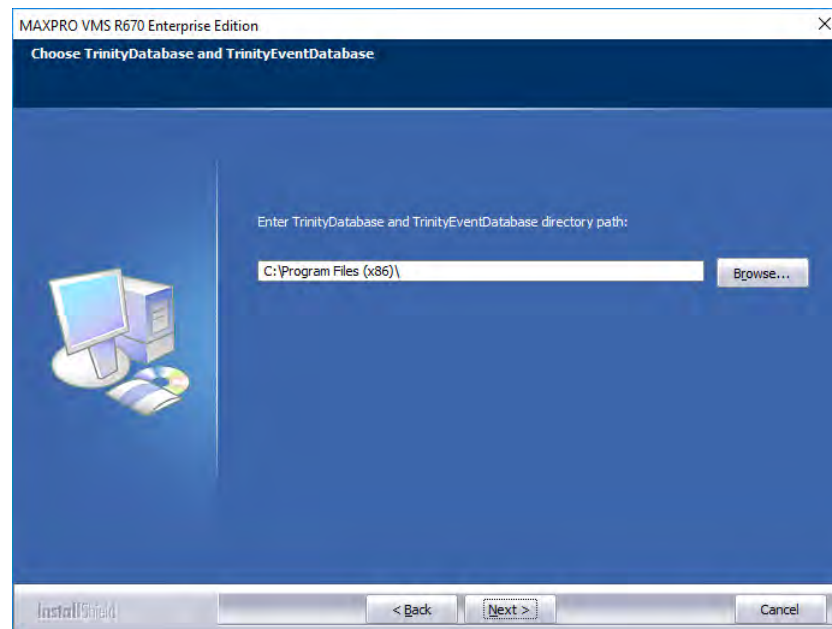


Caution: If the SQL Server Express instance is available on a remote computer and if you do not have sufficient permissions to fetch the instance, then as a result an error message is displayed. In this scenario, the Database Administrator (DBA) must execute some SQL scripts so that instance is fetched. The scripts are available on the installation DVD.

8. Select Connect using option as Windows authentication or SQL Server authentication using Login ID and password below as per the requirement, and then click Next. You are prompted to install SQL Server 2019 Express.

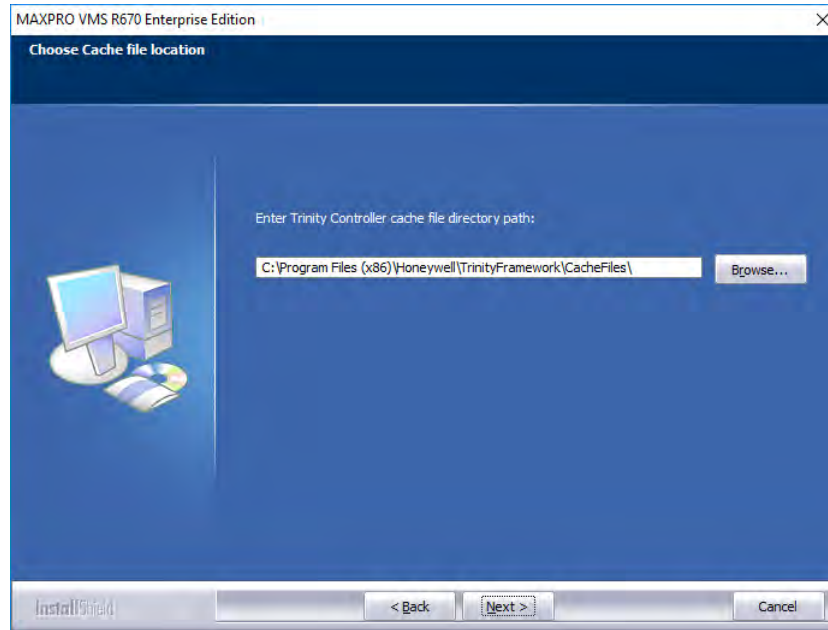


9. Click Yes. The Choose TrinityDatabase and TrinityEventDatabase location dialog box appears.



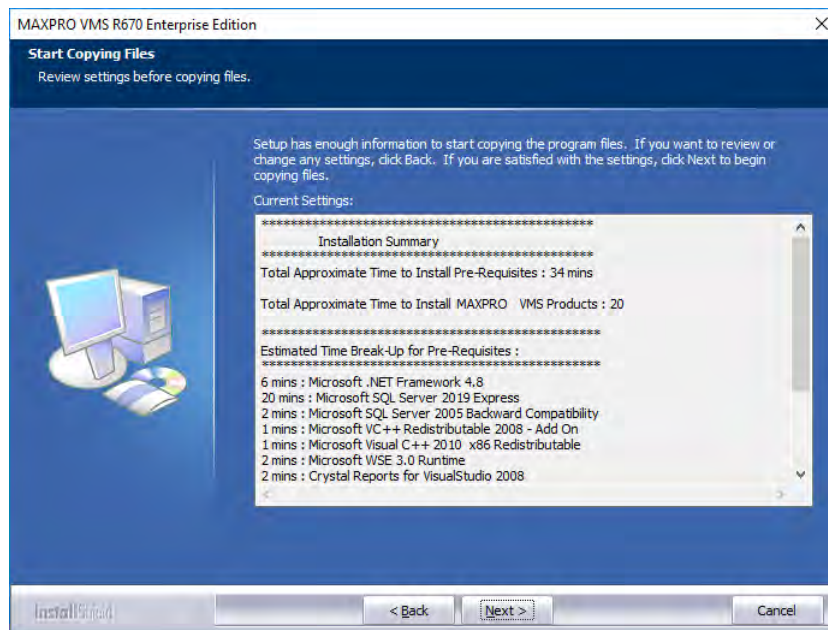
Note: Click Browse to change the default destination folder, and then select the folder where the Trinity database server must be installed. It is best practice to Install the Database on a separate Mirrored hard drive. This ensures the database is still available if the OS drive is failed or get corrupted.

10. Click Next. The Choose Cache file location dialog box appears.



Note: Click Browse to change the default destination folder, and then select the folder where the cache files must be installed.

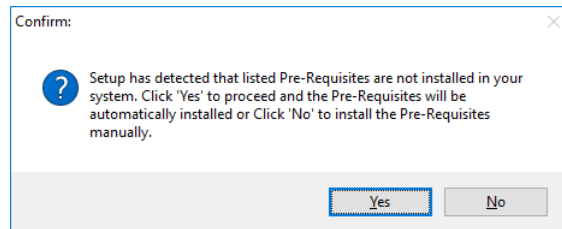
11. Click Next. The Start Copying Files page appears.



12. If you want to review or change any settings click Back.

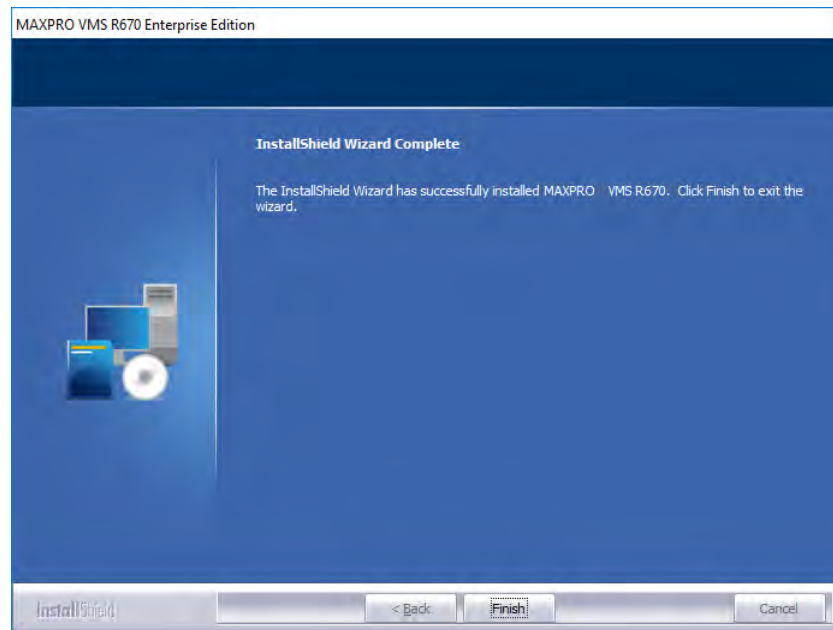
Note: The Start Copying Files page displays the total approximate time for installing the prerequisites and total approximate time for installing the MAXPRO VMS R670 components. Please note that prerequisites take more time for installation than the MAXPRO VMS R670 components.

13. Click Next. The following message appears.



14. Click Yes to install the prerequisites automatically, else click No. From step 15 onwards till the end of the installation, the prerequisites and MAXPRO VMS components are installed automatically without requiring any manual intervention. In addition VC++ 2008 redistributable will be installed as a prerequisite as part of MAXPRO VMS installation.

15. After all the prerequisites and MAXPRO VMS R670 components are successfully installed, the InstallShield Wizard Complete page appears.



16. Click Finish. Your computer reboots. The installation is complete after the reboot operation.

Custom Installation

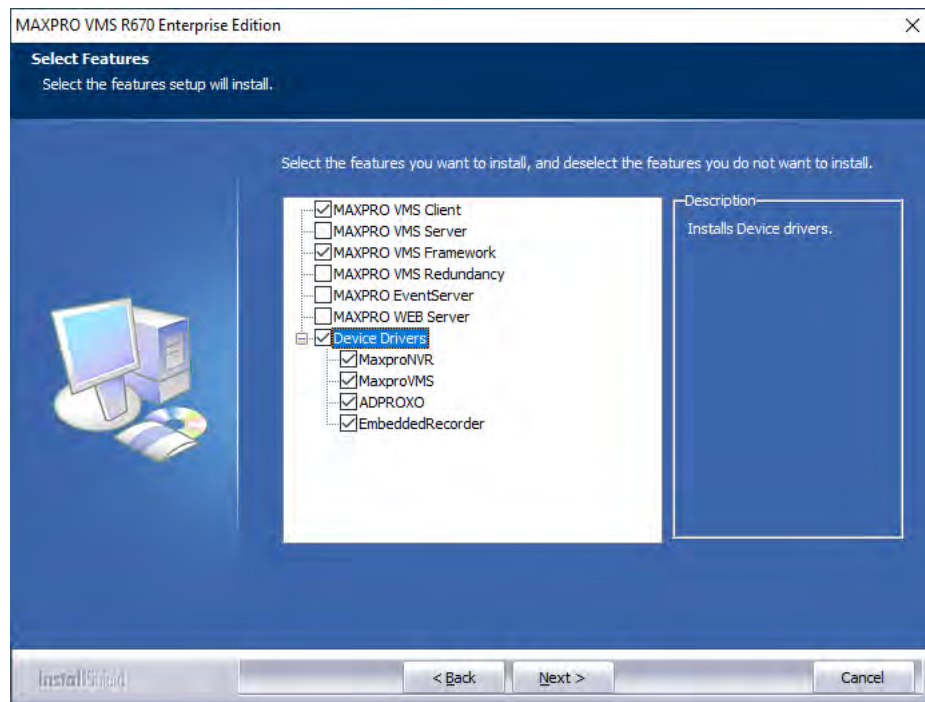
Custom installation gives you an option to install the server and client. You can choose to install various device drivers. The following table lists installation you can do using the custom installation option.

Select features to install

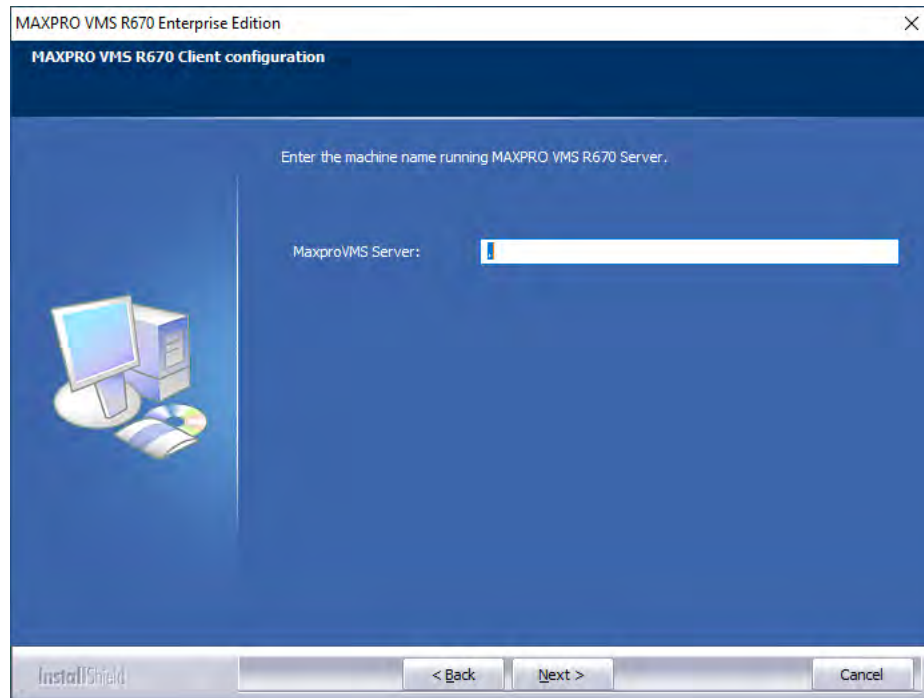
Client	MAXPRO VMS client and MAXPRO VMS Framework are installed. See Installing Client .
Server	MAXPRO VMS server and device drivers are installed. See Complete Installation .

Installing Client

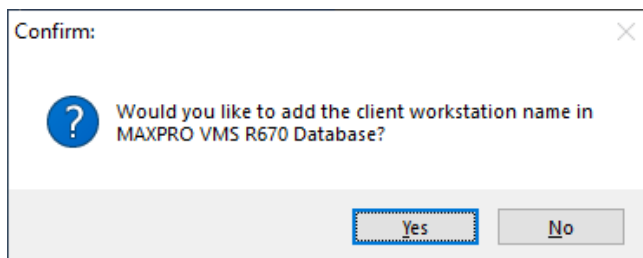
1. Perform steps 1 through 10 in the section [How to Install MAXPRO™ VMS R670](#). The Installation Type page appears.
2. Select Custom Installation, and then click Next. The Select Features dialog box appears.
3. Select the MAXPRO VMS Client check boxes along with required Drivers.



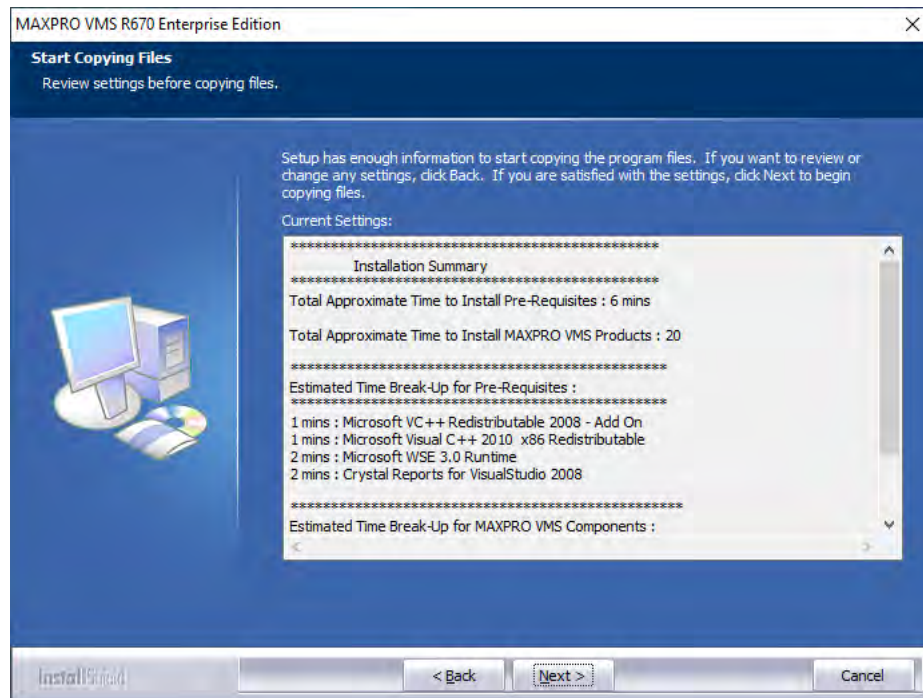
4. Click Next. Client configuration wizard appears.



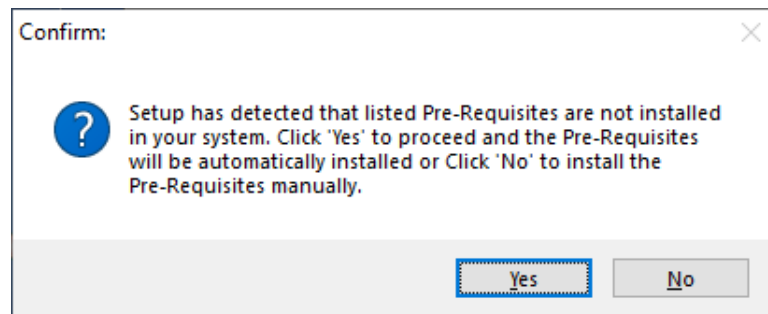
5. Click Next. A Confirmation message appears as shown below.



6. You can do any one of the following:
 - a. Click Yes. The Database Server Login dialog box appears. Enter the details to connect the database and then click Next. Continue from step 7.
 - b. Click No. The Start Copying Files page appears
7. Click Browse, and then select any existing SQL database. You can select the existing SQL database on the same network. If you do not want to select an existing database.
Or
If you want to retain the existing Trinity Database, select Local from the Database Server drop-down and then click Next. A message Do you want to retain the Trinity Database? is displayed click Yes.
8. Select Connect using option as Windows authentication or SQL Server authentication using Login ID and password below as per the requirement, and then click Next. The Start Copying Files page appears.

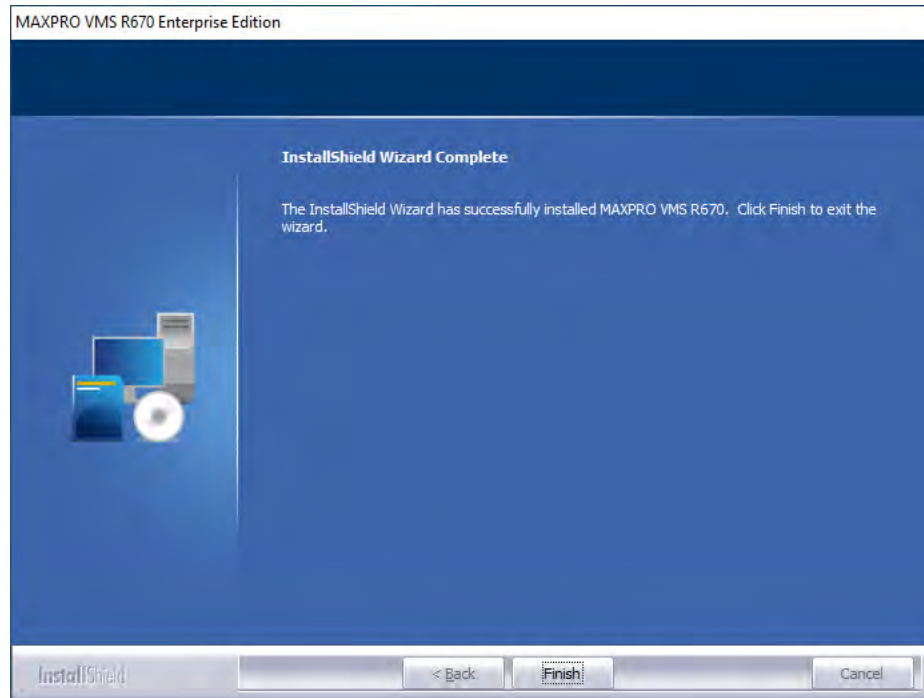


9. If you want to make any changes click Back. Click Next. The following confirmation message is displayed.



10. Click Yes. The MAXPRO VMS installation wizard displays the installation progress. During Installation the reboot confirmation message is displayed. Click OK to reboot the system. Once reboot is done perform the following
 - a. login to the system with credentials.
 - b. If the installation wizard is displayed then click Next to proceed with the installation.
Or
If the installation wizard is not displayed then run the Setup.exe and then click Next to continue with the installation.

Once the installation is completed, the InstallShield Wizard Complete screen appears as shown below.



11. Click Finish. The computer restarts and the installation is complete.

Uninstall the MAXPRO VMS R670 Software

You can remove the MAXPRO VMS R670 completely or some of its components as per your requirements.

Before you begin

1. Stop Trinity Analytics Services.
 - a. Choose **Start>Run**, and then type **services.msc**. The **Services** window appears.
 - b. Right-click **Trinity Analytics Service**, and then select **Stop**.
2. Stop Trinity Services.
 - a. Choose **Start>Run**, and then type **services.msc**. The **Services** window appears.
 - b. Right-click **TrinityController**, and then select **Stop**.
 - c. Right-click **TrinityServer**, and then select **Stop**.

To uninstall MAXPRO VMS R670 completely

1. Insert the MAXPRO VMS R670 setup DVD in the DVD drive, browse to the MAXPRO VMS R600 setup folder, and then double-click Setup.exe or Go to the MAXPRO VMS R600 setup folder in your computer, and then double-click Setup.exe. The Setup Type dialog box appears.

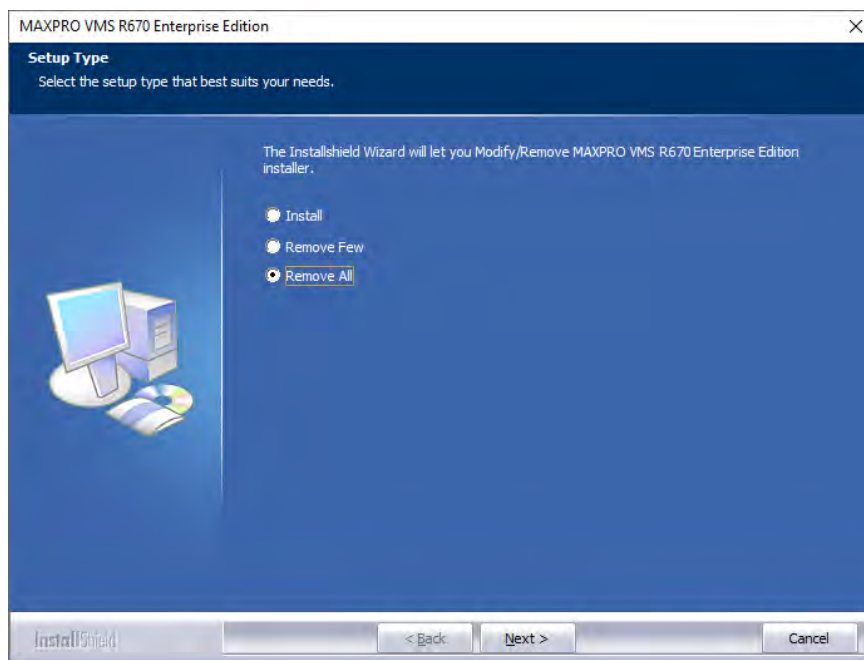


Figure 3-1 Setup Type

2. Select Remove All, and then click Next. The following confirmation message appears.

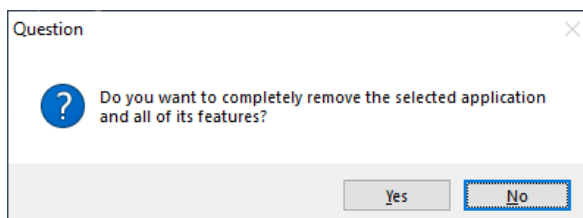


Figure 3-2 Confirmation Message

3. Click Yes. The Restoring Trinity Database page appears.

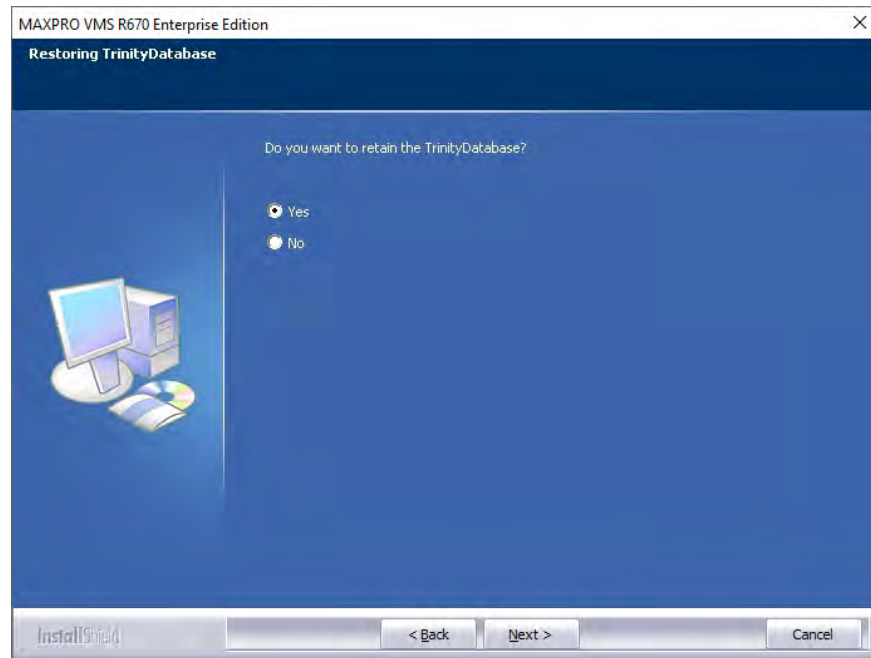


Figure 3-3 Restoring Trinity Database

4. Click Yes to retain the Trinity database and click No to delete the Trinity database. Click Next, the Restoring Analytics Database page appears.

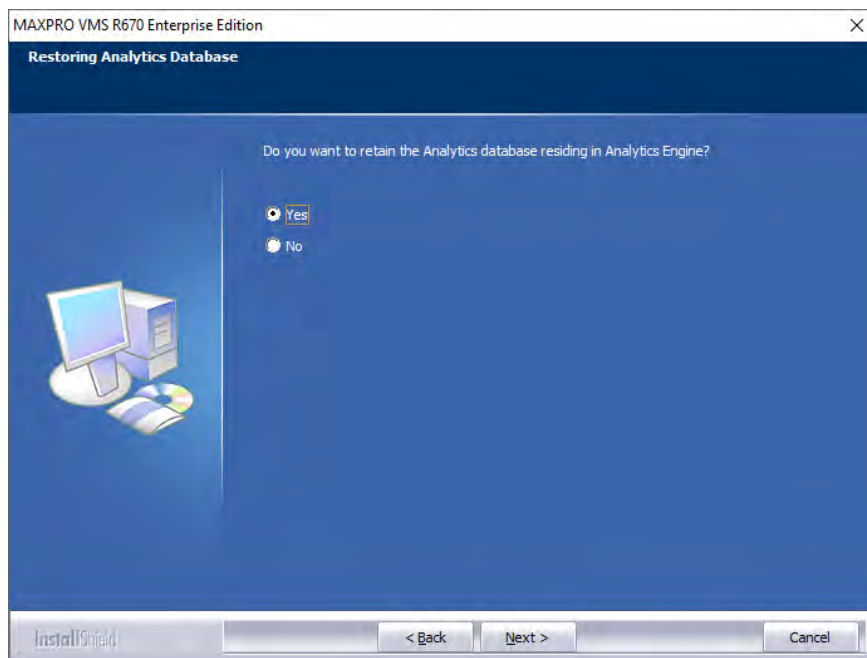


Figure 3-4 Restoring Analytics Database

Note: Despite you select Yes or No to retain Analytics Database, you have to configure the HVA once again after uninstallation.

5. Click Next. The MAXPRO VMS R600 is removed completely and Uninstall Complete page appears.

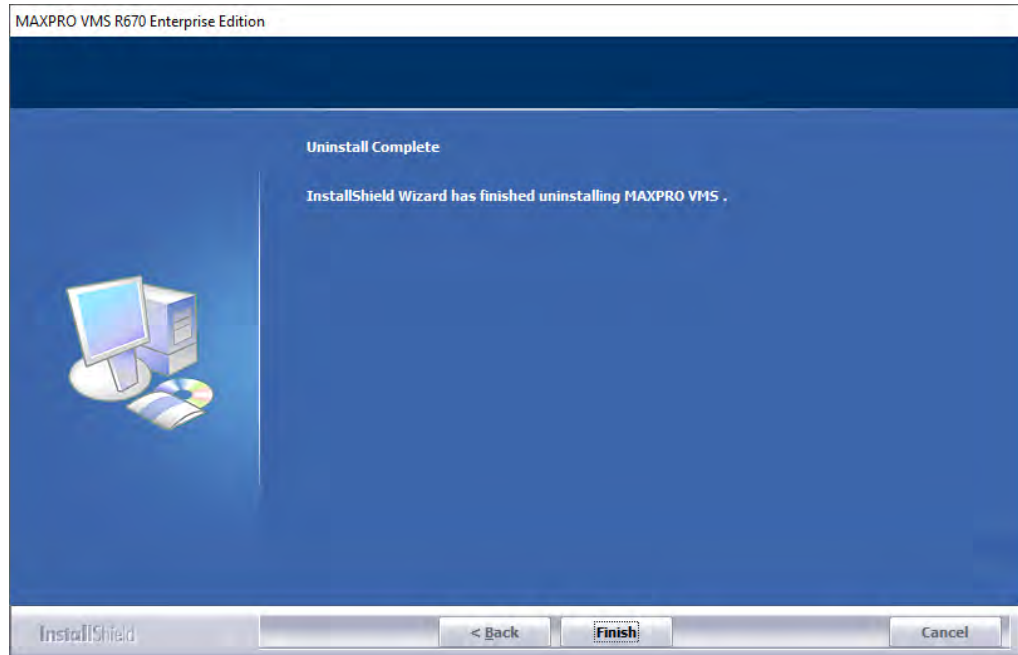


Figure 3-5 Uninstall Complete

6. Click Finish. You are prompted to reboot the computer.

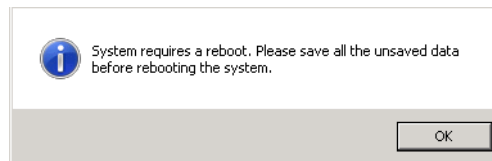


Figure 3-6 Prompt to reboot

7. Click OK.

To uninstall few components

1. Insert the MAXPRO VMS R600 setup DVD in the DVD drive, browse to the MAXPRO VMS R600 setup folder, and then double-click Setup.exe or go to the MAXPRO VMS R600 setup folder in your computer, and then double-click Setup.exe. The Setup Type page appears.

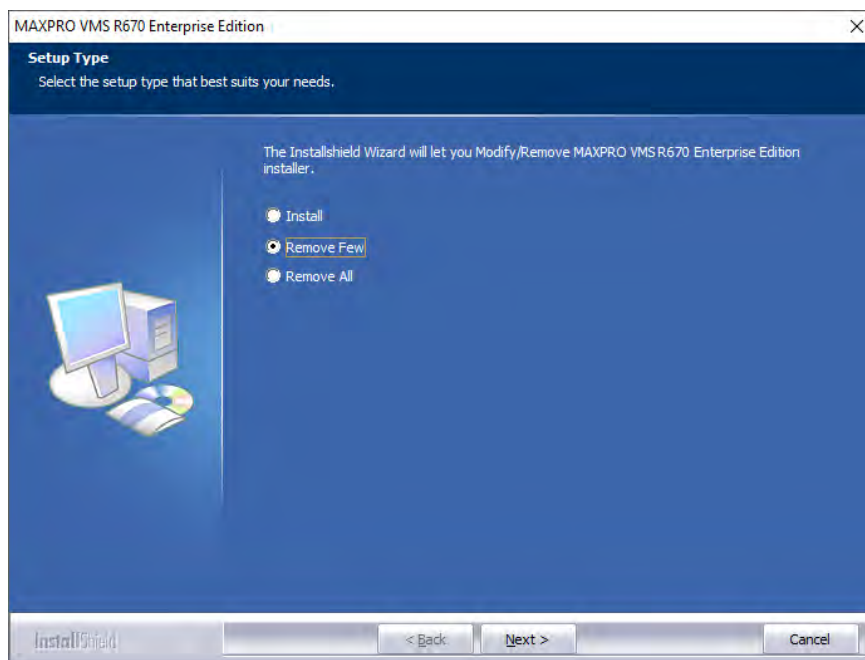


Figure 3-7 Setup Type

2. Select Remove Few, and then click Next. The Select the features dialog box similar to the following figure appears.

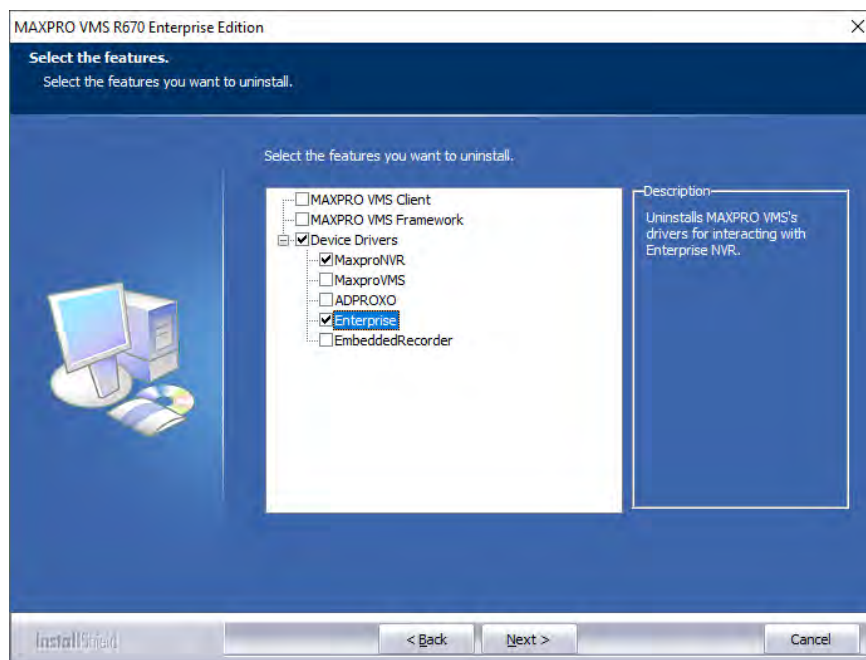


Figure 3-8 Select the Features

Note: Removing Redundancy feature alone is not supported. You should select MAXPRO VMS Server to remove Redundancy feature.

3. Select the components that you wish to remove by selecting the respective check boxes. If you select the Analytics driver to uninstall and click Next then Restoring Analytics Database figure appears as shown below.

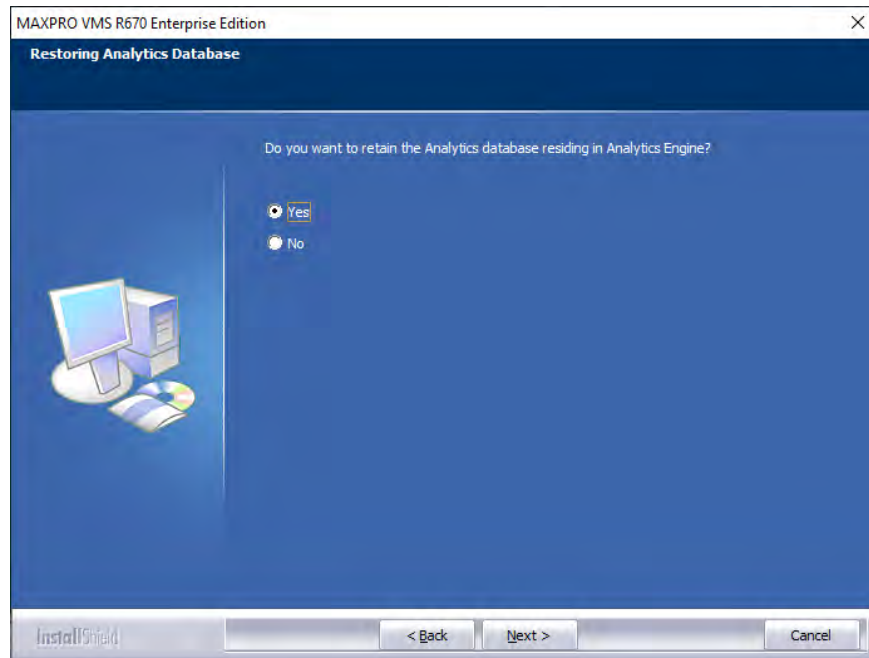


Figure 3-9 Restoring Analytics Database

Note: Despite you select Yes or No to retain Analytics Database, you have to configure the HVA once again after uninstallation.

4. Click the required option to retain the Analytics database residing in Analytics Engine, and then Click Next. The Start Copying Files page similar to the following figure appears.

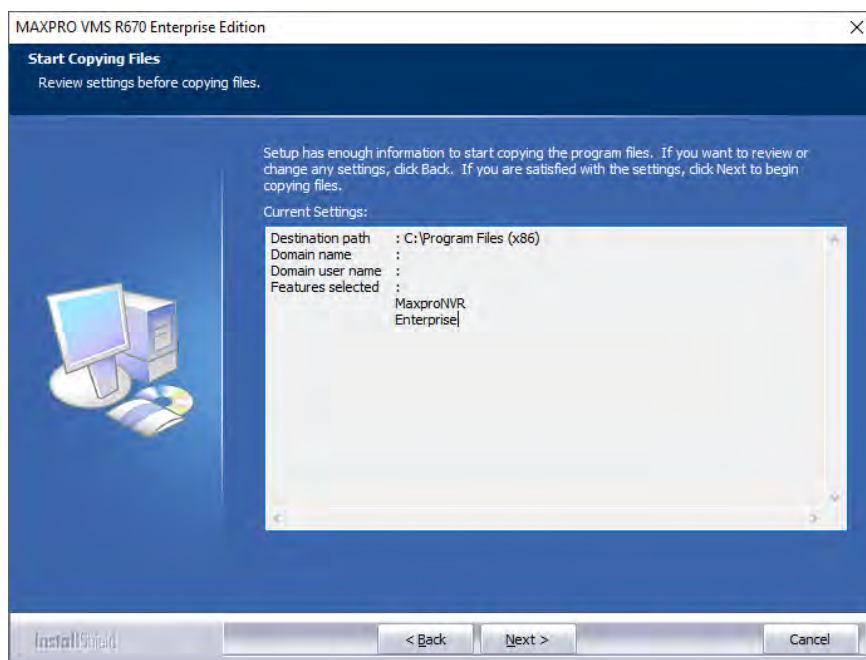
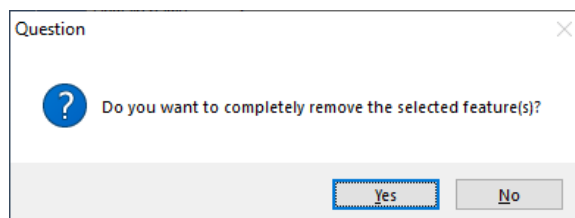


Figure 3-10 Start Copying Files

5. Click Next. A confirmation message appears as shown below.



- Click Yes to proceed. The selected components of the MAXPRO VMS R600 are removed and the Uninstall Complete page appears.

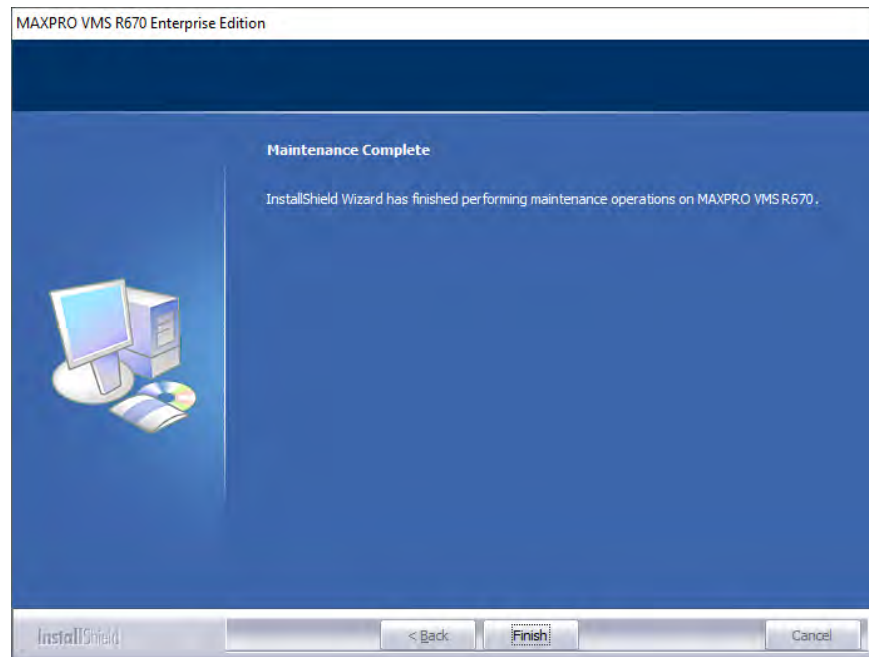


Figure 3-11 Uninstall Complete

- Click Finish. You are prompted to reboot the computer.

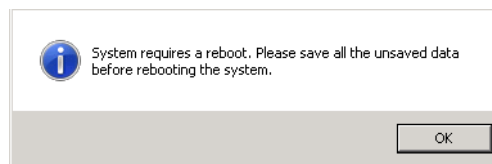


Figure 3-12 Prompt to reboot the computer

- Click OK.

Note: You can remove the required component using the Add or Remove Programs in Windows. However, Honeywell recommends to follow the above mentioned steps to remove MAXPRO VMS R670 components.

After removing MAXPRO VMS

After removing MAXPRO VMS, you must remove Microsoft Loopback Adapter manually.

To remove loopback adapter

1. Right-click My Computer, and then select Properties. The System Properties screen appears.

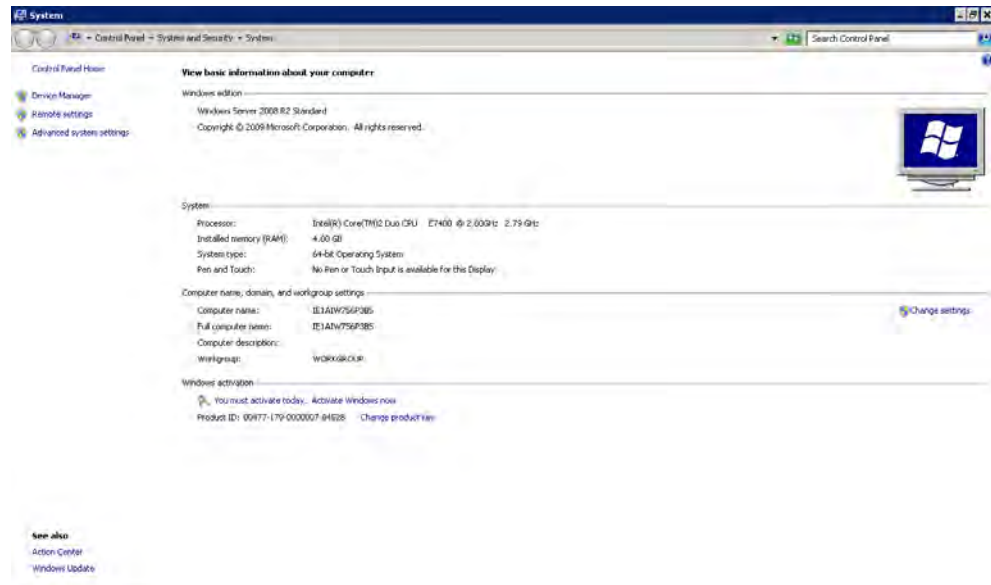


Figure 3-13 System Properties

2. Click Device Manager. The Device Manager screen appears.

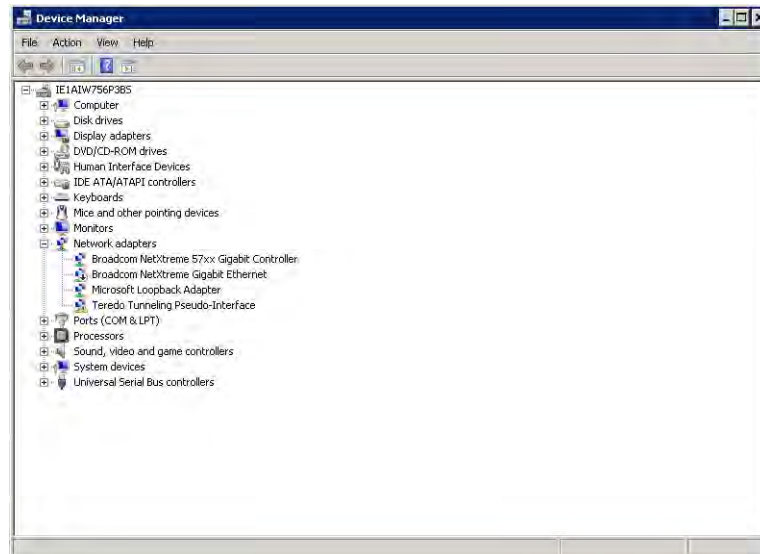


Figure 3-14 Device Manager

- Expand the Network Adapter branch, right-click Microsoft Loopback Adapter, and then select Uninstall. The Confirm Device Removal message box appears.

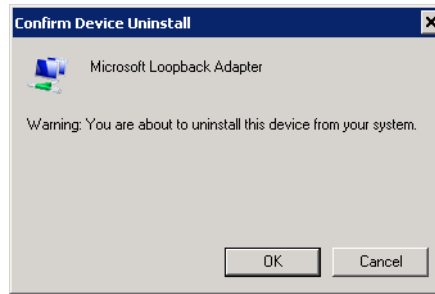



Figure 3-15 Confirm Device Removal


- Click OK.

SQL Express 2014 Sp1 Scenarios

The following table depicts the various scenarios of SQL Express 2014 Sp1 while installing the VMS R600.

Table 2-1 SQL Express 2014 SP1 Scenarios

R600 Installation Scenarios	SQL 2014 SP1 Express Supported OS	SQL 2014 SP1 Express Unsupported OS (If operating system service pack is not installed then)
If you choose for Fresh installation and Server is Selected without SQL instance.	Installs the SQL Express 2014 SP1 and Create Database.	It displays an error message as shown below. 
If you choose for Fresh installation and Server is selected + local SQL Standard Edition instance is selected.	Creates the Database in the selected SQL Standard instance of any version.	Create Database in the selected SQL Standard instance of any version.
If you choose for Fresh installation and Server is Selected + local SQL Express 2008 R2.	Installs the SQL 2008 R2 SP1 (If Required) and Upgrade to SQL Express 2014 SP1 + Upgrade Database.	Create Database in SQL Express 2008 R2 instance.
If you choose for Fresh installation and Server is Selected + local SQL Express 2014 SP1.	Creates the Database. Installs the SQL 2012 R2 SP1/SP2/ Sp3 (If Required) and Upgrade to SQL Express 2014 SP1 + Upgrade Database.	This scenario is not possible.

If you choose for Fresh installation and Server is selected + Remote SQL.	Creates the Database.	Create Database.
If you choose for Fresh installation and Client is selected.	Client components will be installed.	Client components will be installed.
If you Upgrade from R300 Server to R600.	Upgrades to SQL Express 2014 SP1, if R300 has SQL 2008 R2 available and upgrade the Database.	Only Upgrade the Database (SQL will not be upgraded).
If you Upgrade from R300 Client to R600.	Upgrades the client.	Upgrade the client.
If you Upgrade from R310 Client and Server is selected in R600 with no SQL instance.	Installs the SQL Express 2014 SP1 and create the Database.	It displays an error message as shown below. 

Cleaning the System

The Uninstall Utility allows you to clean all the installed R600 components in the system. Uninstall Utility is available in the installation path of VMS R600 under Tools folder. It contains the Database Files, SQL Scripts that allows you to clean the specific component. After you clean the system you need to reinstall the R600 software.

Note: Use this utility, if uninstallation is not done properly.

To access and run the utility

- Browse the MAXPRO VMS R600 installation path for example C:\Program Files (x86)\Honeywell\TrinityFramework\Tools\UninstallUtility folder and double-click the UninstallUtility.exe. MAXPRO VMS Uninstall Utility window appears and displays the progress of cleaning.



Adding the rights to the local administrator account

After installing the SQL 2008 R2, 2012 or 2014 SP1 Express, the Installation fails to start the SQL service on Windows 2008 R2 machine. The following error message is displayed in the Event viewer:

FileMgr::StartLogFiles: Operating system error 2 (The system cannot find the file specified.) occurred while creating or opening file 'e:\sql10_main_t.obj.x86-fre\sql\mkmastr\databases\objfre\i386\MSDBLog.ldf'. Diagnose and correct the operating system error, and retry the operation.

Cause

This issue is by design and occurs because of the account that is running SQL Server Setup does not have one or all of the following rights:

- The right to back up files and directories,
- The right to manage auditing and the security log and
- The right to debug programs.

Resolution

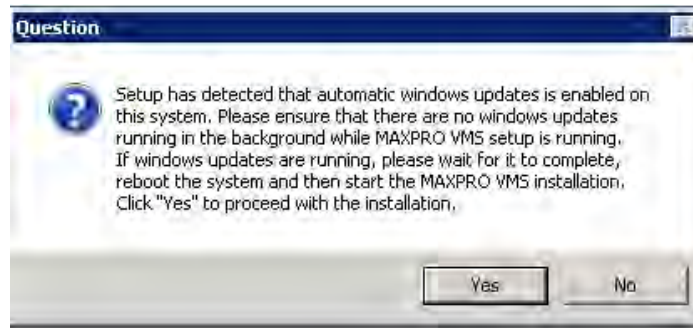
The Setup user account requires the above default user rights for the Setup to be completed successfully.

To add the rights to the local administrator account

1. Log on to the computer as an administrator.
2. Click Start >Run, the Run command window appears.
3. Type Control admintools, and then click OK.
4. Double-click Local Security Policy, the Local Security Settings dialog box appears.
5. Click Local Policies, double-click User Rights Assignment, and then double-click Backup Files and Directories. The Backup Files and Directories Properties dialog box appears.
6. Click Add User or Group. The Select User or Groups dialog box appears.
7. Type the user account that is being used for setup, and then click OK two times.
8. Repeat steps 1 through 7 for the other two policies that are mentioned in the Cause" section.
9. On the File menu, click Exit to close the Local Security Settings dialog box.

Windows Updates

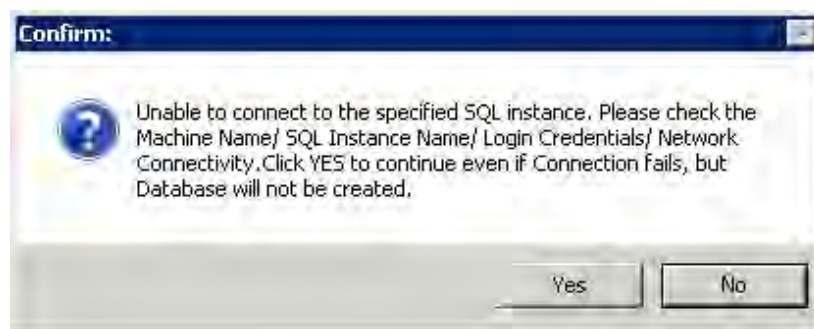
If the windows updates feature is enabled in any of the operating system then while installing MAXPRO VMS R600 the following message is displayed:



User is recommended to wait until the windows updates are installed and then reinstall the VMS R600 software.

Manual Steps if SQL Connection Fails

If the SQL Connection fails, because of invalid credentials entered in the SQL dialog box or for various reasons such as network problems, then the install wizard displays the following message:



If you click Yes and complete the installation then you must perform the following manual steps to work with the application.

1. Update the config files with SQL server and windows/SQL authentication connection details. See [To update the config files](#) .
 - Trinity.SystemServices.exe.config
 - Trinity.ServiceHost.Scheduler.exe.config
2. Add the registry entries. See [To add the registry entries](#) .
3. Execute the create_trinity_db_R400.bat file.

To update the config files

1. Browse <<INSTALL_PATH>>\Honeywell\TrinityFramework\Bin\Trinity.System-Services.exe.config and then double-click the Trinity.SystemServices.exe.config file.

Note: <<INSTALL_PATH>> should be substituted with the actual path selected during installation.

2. For SQL Authentication:
 - a. In the **User ID** field, type the user ID. The default user name is “sa”
 - b. In the **Password** field, type the password. The default user name is “Password1”
 - c. In the **Data Source** field, type “.\SQLEXPRESS”
3. For Windows authentication:
 - In the Server field, type .\SQLExpress.
4. Similarly browse <<INSTALL_PATH>>\Honeywell\TrinityFramework\Bin\Trinity.ServiceHost.Scheduler.exe.config and then double-click the Trinity.ServiceHost.Scheduler.exe.config file.
5. Repeat the steps 2 and 3 to update the config file with SQL Authentication and Windows authentication.

To add the registry entries

1. Access the registry: [HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Honeywell\TrinityFramework].
2. Update the registry value names with the SQL instance details which you are planning to use:

Registry value Name	Value
TRINITYDATABASEPATH=	"c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS64BIT\MSSQL\DATA" TRINITYDATABASEPATH should be replaced with the path fetched from the registry, apart from the selected SQL instance name's DATA path where mdf and ldf files will be stored.
TRINITYDBSERVER=	"admin-PCVMS\SQLEXPRESS64BIT"

3. Similarly access the registry:
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Honeywell\TrinityFramework\DatabaseDetails]

4. Update the registry value names with the SQL instance details which you are planning to use:

Registry value Name	Value
"PCNAME"=	"admin-PCVMS"
"CONNECTIONSTRING"=	"Persist Security Info=False;User ID=sa;Password=Password1;Initial Catalog=TrinityDatabase;Data Source=admin-PCVMS\SQLEXPRESS64BIT"
"DATABASEPATH"=	"c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS64BIT\MSSQL\DATA" DATABASEPATH should be replaced with the path fetched from the registry, apart from the selected SQL instance name's DATA path where MDF and LDF files will be stored.
"INSTANCENAME"=	"SQLEXPRESS64BIT"
"PASSWORD"=	"9bvmw?"
"TRINITYDBSERVER"=	"admin-PCVMS\SQLEXPRESS64BIT"
"SQLMODE"=	"1"
"USER"=	"sa"
"TRINITYDATABASEPATH"=	"c:\Program Files\Microsoft SQL Server\MSSQL11.SQLEXPRESS64BIT\MSSQL\DATA"

Note: If you are using 32 bit Operating System then you should not access the Wow6432 Node.

Executing the create_trinity_db_R400.bat file

Prerequisites

Ensure that you have updated the config files and added the registry entries as explained in [To update the config files](#) and [To add the registry entries](#).

To execute the "create_trinity_db_R400.bat" file

1. Browse the "create_trinity_db_R400.bat" file in the Tools folder available in the setup media.
2. Right-click the "create_trinity_db_R400.bat" file and then select Run as Administrator. If you have selected SQL authentication then the execution prompts for SQL server name, windows authentication option or SQL authentication option, user name and password.
3. Provide the necessary details. The TrinityDatabase is created.

Honeywell Intelligent Command Installation

The Intelligent Command is a web based application that allows access to certain MAXPRO functionalities remotely from any location.

The functional hierarchy of the MAXPRO Intelligent Command, MAXPRO Web API and MAXPRO Server are as follows:

1. The Intelligent Command sends a request to the MAXPRO Web API.
2. The MAXPRO Web API interacts with MAXPRO Server and processes the request.
3. Finally the result of request is sent back to the MAXPRO Intelligent Command.

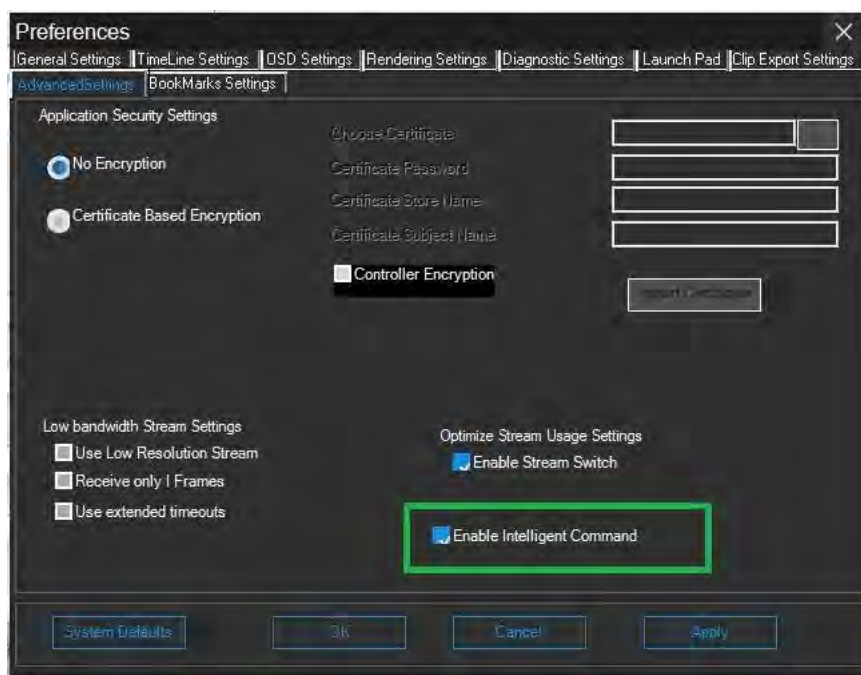
Refer to the 800-26663-A_IC R670 Installation Guide for complete detail on how to install Honeywell Intelligent Command.

Enabling Intelligent Command in VMS

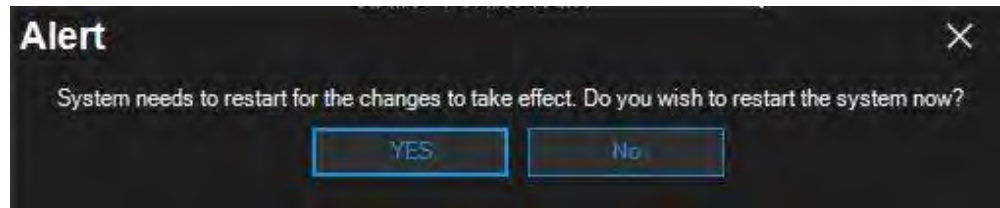
After installing VMS R670, user should enable the Intelligent command option to use the IC features.

Note: Without enabling this option, user cannot see the Intelligent command option in VMS.

1. In VMS Preferences > Advanced settings tab, select the Enable Intelligent Command as shown below.



2. Click Apply and then OK. A message to restart the PC is displayed.



3. Click Yes to restart the PC for the changes to take effect.

CONFIGURING DEVICES AND SETTING UP A SITE

Overview

Configuring MAXPRO VMS involves setting up the application to perform surveillance operations. This is the most important phase for commissioning MAXPRO VMS as it involves organizing devices, users, and roles associated to them.


Before you begin

- Ensure that you have completed MAXPRO VMS server and client hardware setup and software installation.
- Configure the firewall settings as mentioned in the Firewall Settings section.

Configuring MAXPRO VMS

You can configure the MAXPRO VMS using the Configurator tab in the user interface. The navigation area inside the Configurator tab helps you to configure devices, groups, and manage users and roles.

To go to configurator tab

1. Double-click the icon  on your desktop. The Log On page appears.

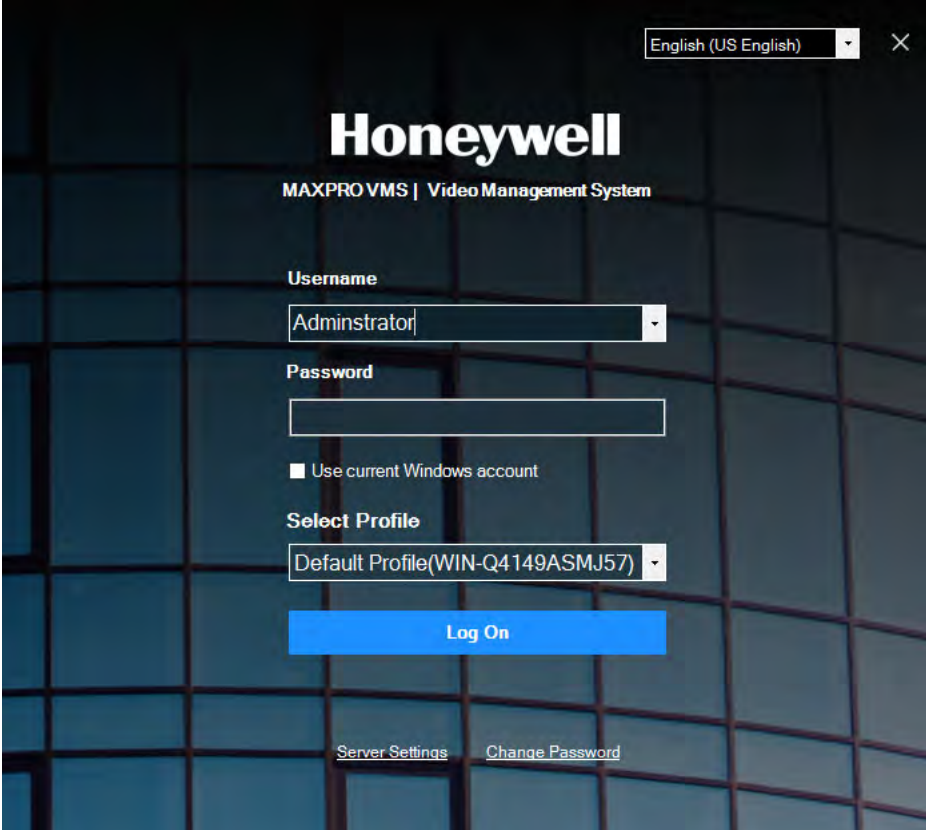
The image shows the Honeywell MAXPRO VMS Log On interface. At the top right, there is a language dropdown menu set to 'English (US English)' and a close button (X). The Honeywell logo is prominently displayed in the center, with 'MAXPRO VMS | Video Management System' underneath it. Below the logo, there are two input fields: 'Username' with a dropdown menu showing 'Administrator' and 'Password' with a text box. A checkbox labeled 'Use current Windows account' is positioned below the password field. Underneath the checkbox is a 'Select Profile' dropdown menu showing 'Default Profile(WIN-Q4149ASMJ57)'. A large blue 'Log On' button is centered below these fields. At the bottom, there are two links: 'Server Settings' and 'Change Password'.

Figure 4-1 MAXPRO VMS Log on

2. In the Username box, type the user name.
3. In the Password box, type the configured password.

Note: Select the Use current Windows account check box to log on using the Windows system credentials

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

Note: Honeywell recommends you to change the default Password before you logon to MAXPRO VMS. See [Changing the Default Password](#) section. Refer to [Securing MAXPRO® VMS Technical Notes](#) for further details

4. Click . The Viewer tab appears by default.

5. Click Configurator tab. The Configurator screen appears.

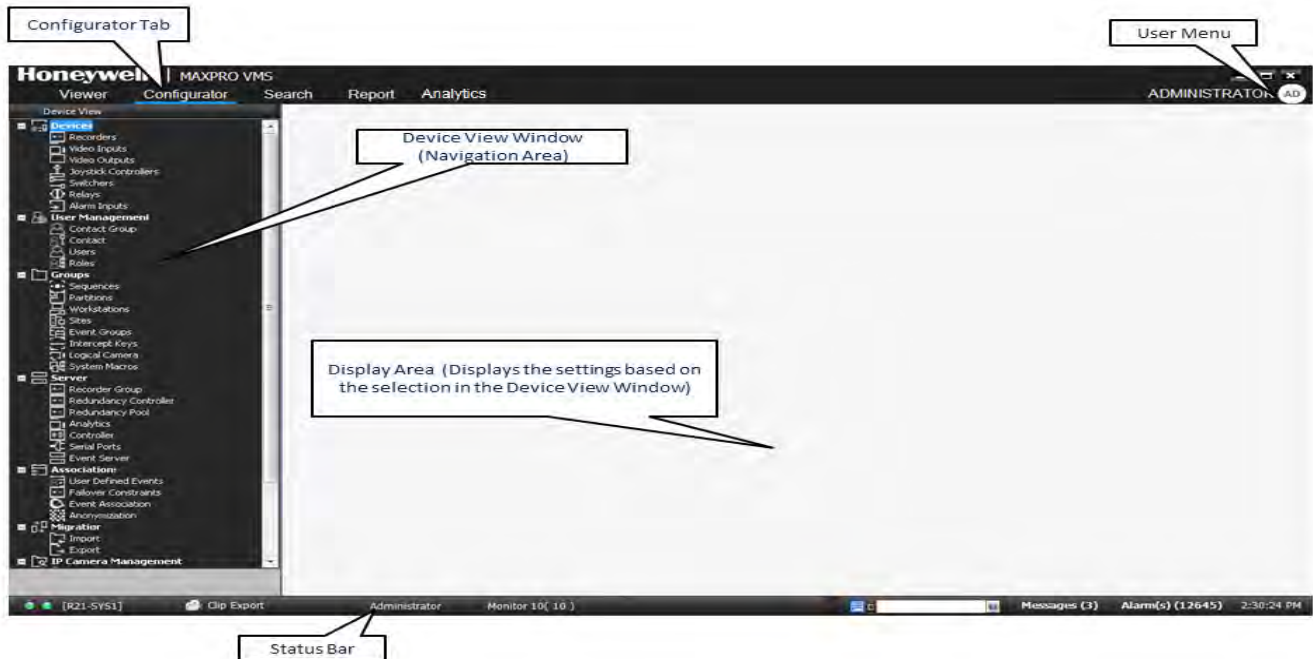


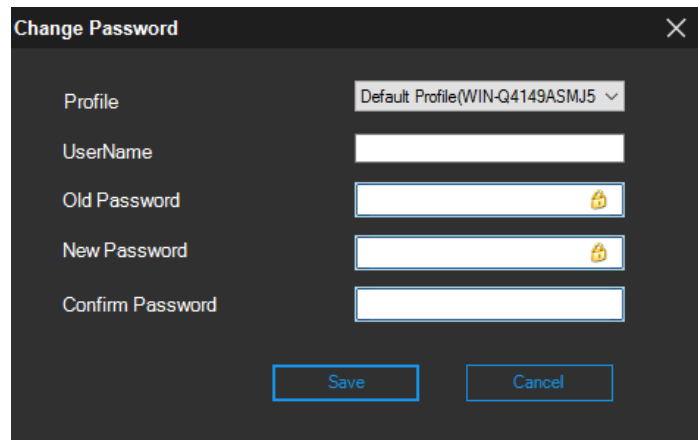
Figure 4-2 Configurator tab

Changing the Default Password

Honeywell recommends you to change the default password and create a new password before logging on to MAXPRO VMS software. Refer to [Securing MAX-PRO® VMS - NVR Technical Notes](#) for further details.

To change the default password:

1. In the client workstation, double-click the  icon in the desktop to display the Log On page.
2. Click Change password. The Change Password page appears.



The image shows a 'Change Password' dialog box with a dark background. It contains the following fields and controls:

- Profile:** A drop-down menu showing 'Default Profile(WIN-Q4149ASMJ5)'.
- UserName:** A text input field.
- Old Password:** A text input field with a lock icon on the right.
- New Password:** A text input field with a lock icon on the right.
- Confirm Password:** A text input field.
- Buttons:** 'Save' and 'Cancel' buttons at the bottom right.

3. Select the Profile from the drop-down list for which you want to change the password.
4. Type the Username. The default username is admin.
5. Type the Old Password

Note: Old password is blank for Fresh installations.
 In upgrade installation, use old password which is configured before upgrade. Refer to [Securing MAXPRO® VMS Technical Notes](#) for further details. Logon as Administrator only when an administrative activity need to be performed, Operator is preferred for all other activity.

6. Type the New password.
7. Type the new password once again to Confirm Password.
8. Click Save.

Password Requirement

Ensure that the new password must meet the following requirements.

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

Setting up a site using Configurator

A site enables you to monitor the activities in an area. Setting up a site involves adding and configuring the hardware devices, defining the users, partitions, recorder groups and event groups.

Setting up a site involves the following:

Adding Sites

A default site is added when you install MAXPRO VMS. You can use the default site and associate the hardware devices to it. You can also create new sites. See [Site](#) for more information.

Adding Workstations

Workstations are client computers in which the MAXPRO VMS user interface is installed. The users can perform actions such as monitoring a site, generating reports, searching for video recording, and configuring (add, update, and delete) devices from these workstations. See [Workstations](#) for more information.

Adding Partitions

A partition is a logical grouping of recorders, cameras, switchers, and monitors in a site. A default partition is added when you install MAXPRO VMS. You can associate the default partition to cameras and recorders or create new partitions. See [Partitions](#) for more information.

Note: Partitions are used to limit user access to devices and cameras.

Adding Roles and Users

A default administrator user with the administrator privileges is created when you install MAXPRO VMS. The privileges for a user are defined in roles. You can define roles according to your requirements and assign them to users. The users are associated to a site. Only the users with access to the site can perform actions such as viewing video, acknowledging alarms, and others based on the user privileges. See [Users](#) and [Roles](#) for more information.

Adding Contact Group and Contacts

You can add a contact group of users with different roles and also store a contact in MAXPRO VMS. An alarm notification can be configured to a contact group. See [Contact Group](#) for more information.

Adding Event Groups

An event group is a grouping of events that occur on devices. The events in each event group are defined when you add a device such as recorder, switcher, and camera. A default event group is added when you install MAXPRO VMS. You can use the default event group or create new event groups. See [Event Group](#) for more information.

Adding Recorder Groups

Recorder group feature distributes the load on a controller. It allows you to create different groups and associate recorders to it. Associating recorders to the groups enables the load is distributed among the recorder controllers. See [Recorder Groups](#) for more information

Adding Serial Ports

Serial ports are added for communication with joystick controllers (Ultrakey keyboards), switchers, and Protocol Interface Translators (PIT). You can add up to 20 serial ports to MAXPRO VMS server. See [Serial Port](#) for more information.

Adding Analytics

You can add analytics server for automating motion detection, triggering real-time alarms, and enabling fast search and retrieval of videos. The applications can be launched directly from the server or from a separate client personal computer (PC) that can access the server through a TCP connection. See [Analytics](#) for more information.

Adding Recorders

You can add MAXPRO NVR, ENVR, ADPRO XO and VMS in VMS recorders in R600. After adding recorders, you can associate them with partitions, and define the events. Only users of the partition that is associated with the recorder can configure the recorder settings. Only the events defined for the recorder can be configured to trigger event based alarms. For example, if you associate Recorder Disconnected event to a recorder, you can configure an alarm to be triggered when this event occurs. See [Recorders](#) for more information.

Adding Switchers

Presently, you can add Vicon, Burle, American Dynamics, Pelco, VideoBlox, and MAXPRO switchers. See "Switchers" on page 5-186.

Adding Video Inputs

You can add video inputs and associate them to recorders and switchers. See [Video Inputs](#) for more information.

Adding Video Outputs

You can add video outputs like standard device, trunk, VCR, analog and digital monitors. See [Video Outputs](#) for more information.

Adding Relays

You can add relays that can be connected to devices like switcher, recorder, cameras, keyboard, and high level device. Relays send signals that perform various actions. For example, you can set a relay to open the door automatically when a motion is detected in a particular region. See [Relays](#) for more information.

Adding Alarm Inputs

You can add alarm input to raise alarms through an external device in MAXPRO VMS. These alarm inputs can be associated to devices like switcher, recorder, cameras, keyboard, networks and high level device. See [Alarm Inputs](#) for more information.

Adding Logical Cameras

You can group the cameras using the logical camera option. Using the logical camera option, selection of a particular camera is made easier. See [Logical Camera](#) for more information.

Adding Sequences

You can define sequences to view live video streamed one after the other from cameras for a specified time interval. See [Sequences](#) for more information.

Adding System Macros

A macro is a rule or pattern that specifies how a certain input sequence (often a sequence of characters) is mapped to an output sequence or action. See [System Macros](#) for more information.

Adding Joystick Controllers

An Ultrakey keyboard is referred to as the joystick controller. Using the Ultrakey keyboard, you can perform actions such as selecting a camera in the Viewer tab. See [Joystick Controllers](#) for more information.

Adding Intercept Keys

Frequently used or repetitive sequence of keystrokes can be automated using intercept keys. Each intercept key is associated with a macro. See [Intercept Keys](#) for more information.

Scheduling

You can schedule an alarm notification, jobs to be performed at a stipulated time, configure SMTP setting, and create an email template in MAXPRO VMS. See [Scheduler](#), [Jobs](#), [SMTP Server Settings](#), [Alarm Notification](#) and [Creating an Email Template](#) for more information.

Recorders

Recorders are devices used for streaming video and recording video from surveillance cameras (analog cameras and IP based digital cameras).

Recorders and Partitions

A partition is a logical grouping of video devices. Partitions are associated to recorders. You can restrict a non-associated user of the partition from viewing or changing the settings of the recorder.

Recorders and Events

Events are predefined actions. Recorders have predefined events by default. An alarm is triggered whenever an event is generated. For example, when a camera is added to a recorder, an event 'CameraAdded' is generated. You can also associate event attributes to events.

Adding a Recorder

Before you begin

- Add Site. See [Adding a Site](#) for more information.
- Add Partition. See [Adding a Partition](#) for more information.
- Add Event Groups. See [Adding an Event Group](#) for more information.

By default, a site, partition and event groups are available. You can associate the recorder to them or create new.

To add a recorder

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Recorders. The Recorders screen appears in the display area.
3. Click Add. The General Settings screen for the recorder appears.

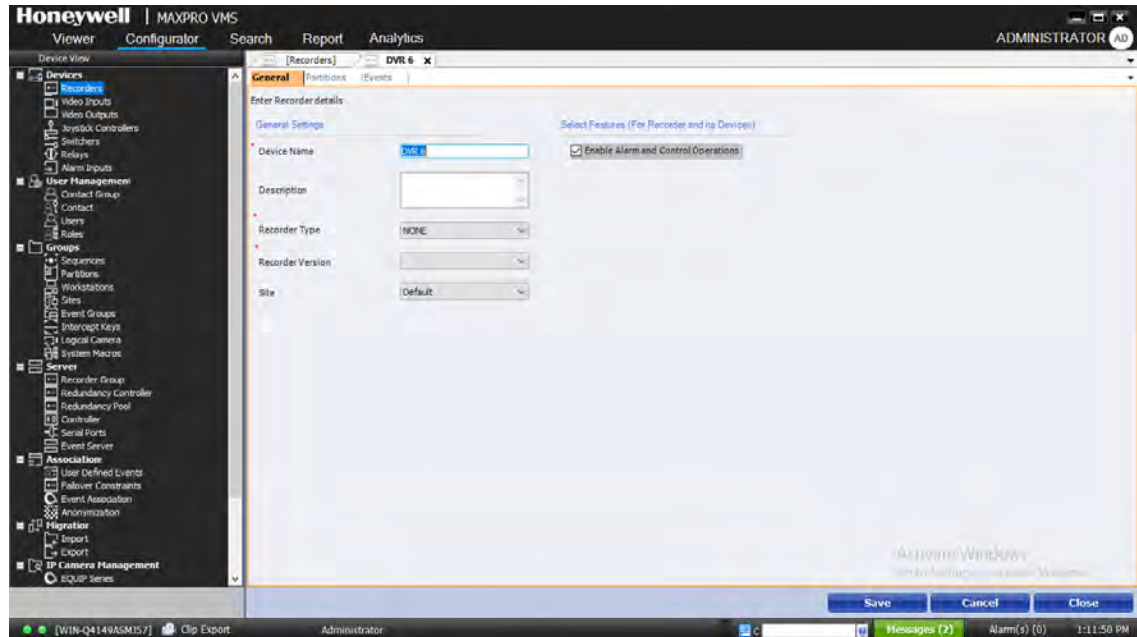


Figure 4-3 Recorder General Settings

4. In the Device Name box, type a name for the recorder. Maximum characters that you can type is 50.
5. In the Description box, type a description for the recorder.
6. In the Recorder Type drop-down list, select the recorder. Device settings for the selected recorder appear. The following table explains how to configure the Device settings for the recorders.
7. In the Recorder Version drop-down list, select the recorder version.
8. In the Site drop-down list, select the site to which the recorder is to be associated.
9. In the Select Features (For Recorder and its Devices), select the check box to enable the Alarm and Control Operations.
10. Associate Partition. See [Discovering Devices](#) for more information.
11. Associate Events and Event Attributes. See [Associating Events and Event Attributes to a Recorder](#) for more information.
12. Click Save.

Recorder Type	To configure the device settings
MAXPRO NVR	<p>In the Unit Address box, type the numeric IP address or the host name of the MAXPRO NVR recorder. Click Ping to verify the connection. The field appears in green if the IP address or the host name is valid.</p> <p>Select the Check for duplicate IP address/ device name in the database check box to check the availability of the host name.</p> <p>In the Site Port box, the port number appears by default.</p> <p>In the Controller Port box, the port number appears by default.</p> <p>In the StorageEngine Port box, the port number appears by default.</p> <p>In the Web Server Port box, the port number appears by default.</p> <p>In the User Name box, the user name appears by default.</p> <p>In the Password box, the password appears by default.</p> <p>Select the Timezone check box to set the timezone. By default it displays the timezone of your location.</p> <p>Under Select Feature (For Recorder and its Devices) perform the following:</p> <p>Select the Enable Alarm and Control Operations check box to enable the alarm and control operations. By default this check is box is selected.</p> <p>Select the Redundant recorder check box if the recorder added is a redundant recorder. Click Save to complete the configuration.</p> <p>If the added recorder is a primary recorder then under Failover/Failback select the Enable check box. By default Automatic option is selected. Click Save to complete the configuration.</p> <p>If you want to trigger the failover manually then select the Manual option. Click Save to complete the configuration.</p> <p>See Configuring Redundancy Controller on page 269. See Configuring Redundancy Pool on page 273. Refer MAXPRO® VMS Operators Guide for more information on Monitoring Redundancy Recorders.</p>
ADPRO XO	Refer to the ADPRO XO Specific documents on how to add and configure ADPRO XO recorder
VMS in VMS	See VMS as a Recorder on page 110 for more information.

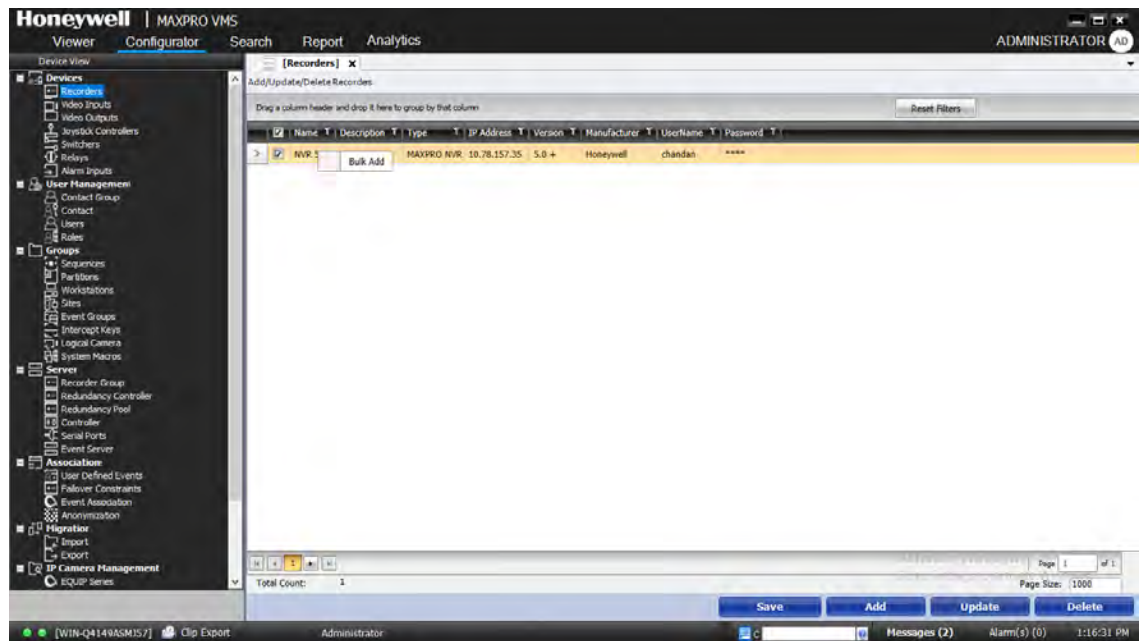
- Click Discover Devices to discover various devices that are connected to MAXPRO VMS. See [Discovering Devices](#) for more information.

Adding Recorder in Bulk

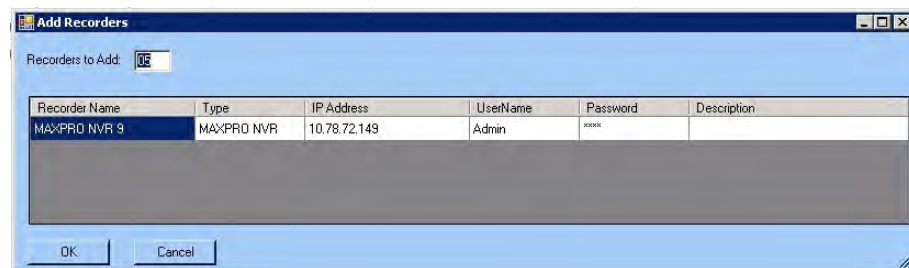
Using Add Bulk feature you can add number of recorder at once.

To add the recorder in bulk

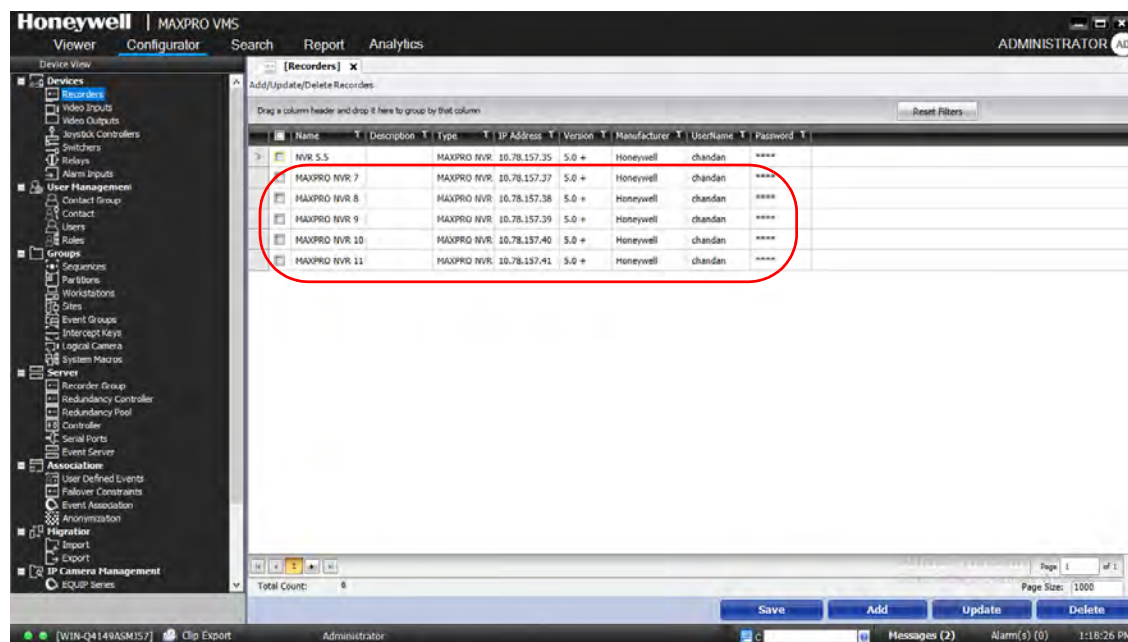
1. In the Recorder screen, select the required recorder check box.
2. Right-click on the selected recorder name and then click Bulk Add as shown below.



The Add Recorders window is displayed as shown below.



3. Type the number of recorder to add in Recorders to Add box and then click OK. The number of new recorders added is highlighted in the recorder screen as shown below.



VMS as a Recorder

This feature is also called “VMS in VMS”. You can configure MAXPRO VMS as recorder similar to any other recorder like Fusion and so on. This configuration is useful if there are more than 10000 MAXPRO VMS's configured in different locations and you want to control them from one master MAXPRO VMS.

For example, there are 3 sites A, B, and C having MAXPRO VMS1, MAXPRO VMS2, MAXPRO VMS3 configured. Here A is considered as the centralized site where the master VMS, MAXPRO VMS1 is configured. In this scenario, you can configure the MAXPRO VMS 2 and MAXPRO VMS 3 as recorders in a MAXPRO VMS1 and monitor the surveillance operations. See [Discovering Devices](#) section on how to discover the recorders.

In VMS R500 release a set of enhancements made for VMS in VMS scenario. Apart from discovering Cameras, relays and sensors user can now discover Sites, Workstations, partitions and users. This feature helps user to import all the configurations from the child VMS to Master VMS instead of reconfiguring it and hence saves time. See [VMS in VMS Enhancements](#) section for more information.

Discovering Devices

Discover devices feature allows you to discover the devices associated to recorders (For example: MAXPRO NVR, ENVR, ADPRO XO and VMS in VMS). In addition you can also discover Sites, Workstations, partitions and users. This helps user to import all the configurations from the child VMS to Master VMS instead of reconfiguring it and hence saves time.

To discover recorder devices

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Recorders. The Recorders screen appears in the display area.
3. Double-click the check box corresponding to the recorder from which you want to discover devices. The Recorder details screen appear. By default General tab is selected.
4. Select the required recorder from the Recorder Type. The Device Settings pane is displayed.
5. Click Discover Devices. The Discovery Wizard page appears.

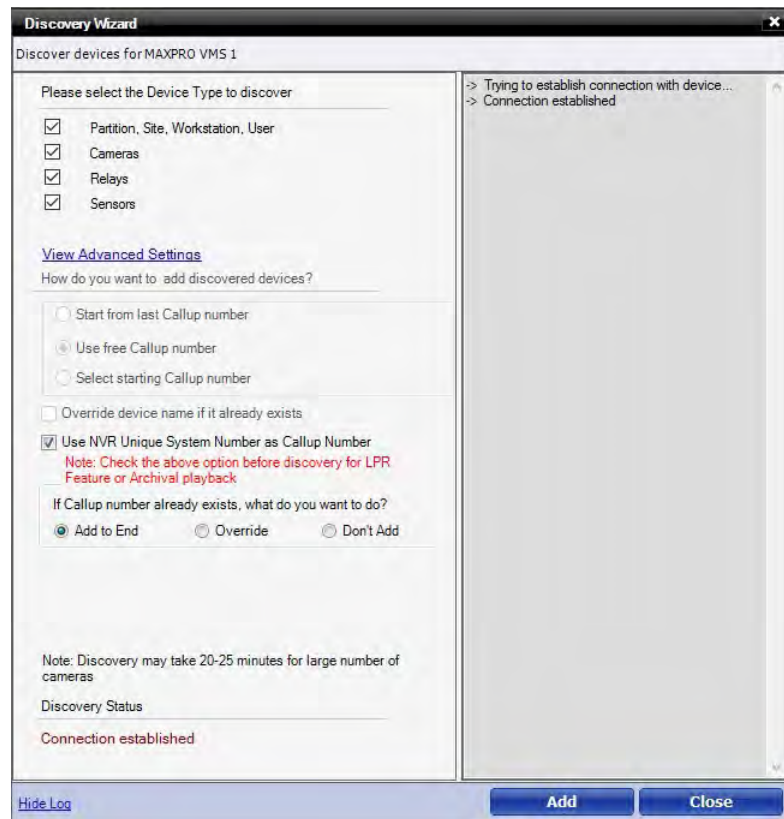


Figure 4-4 Discovery Wizard

6. Select the device or devices that you want to discover.
7. Click View Advanced Settings to configure advanced settings and to specify the order of discovered devices.

Settings	Instruction
Start from last Callup number	Select this option if you want to add the device from the last callup number of the device type that has been selected.
Use free Callup number	Select this option to use the available callup number in the device type that has been selected.

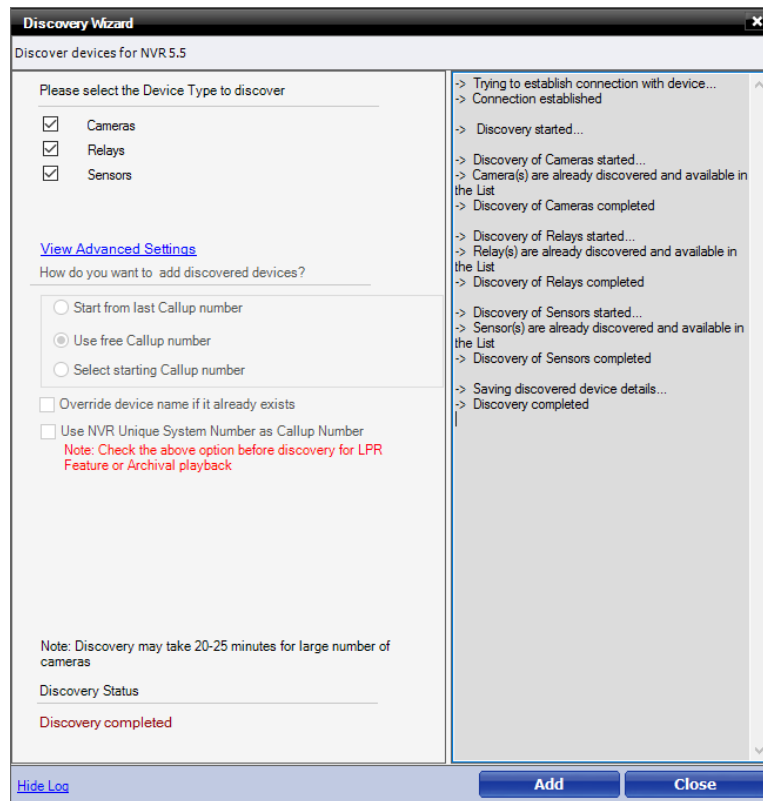
Settings	Instruction
Select starting Callup number	Type the starting callup number, and then choose an option from If Callup number already exists, what do you want to do? section. See step 8 .
Override device name if it already exists	Select the option to override the device name that already exists.
Use NVR Unique System Number as Callup Number	Select the option to use the same callup number of MAXPRO NVR. When this option is selected, choose the options from If Callup number already exists, what do you want to do? section and Camera Type Selection . See step 8 . Before discovering the devices select this check box to experience smooth process for LPR feature and Archival Playback.
Use Enterprise System Number as Callup Number	Select the option to use the same callup number of Enterprise. When this option is selected, choose the options from If Callup number already exists, what do you want to do? section and Camera Type Selection . See step 8 and step 9 .
Use Child VMS Callup Number as Callup Number	This feature is applicable only for MAXPRO VMS recorder. Select the option to use the same callup number of the cameras configured in the child VMS. When this option is selected, choose the options from If Callup number already exists, what do you want to do? section. See step 8 .

8. In If Callup number already exists, what do you want to do? selection, select the required option. The available options are:
 - Add to End - appends to the end of existing call up number.
 - Override - overrides the callup number.
 - Don't Add - does not add the callup number
9. In Camera Type Selection section, select Add Camera as Digital Camera or Add Camera as Hybrid Camera.
10. Click View Discover Log to view any log.
11. Click Close once connection established status appears in Discovery Status section.

Note: All the cameras connected to the recorders would be added. The list of cameras appear in the Site window in the Devices tab. You can select the cameras that you want to add and the Camera Server, Video Clip Directory and Video Format.

To discover the cameras, Relays, Sensors:

- In Discovery Wizard, click the Add. The discovery progress starts on the right pane. Once the discovery completes, the status is displayed as shown below.



To discover cameras connected to recorders (such as MAXPRO NVR)

1. In Discovery Wizard, click the Add. The Discover IP Cameras (Axis/Equip) page appears.

Discover IP Cameras (Axis/Equip)

Step 1: Select Cameras to Add to IPEngine

Streamer ...	Name	IP Address	Streamer Video...	Status	MAC /	
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.76	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.86	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.84	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.80	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.85	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.82	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.77	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.79	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.81	-1	Could not resol...	0040
<input type="checkbox"/>	Could not ...	AXIS Q7406 Ch...	159.99.186.75	-1	Could not resol...	0040

Refresh

Step 2: Please select the Site

Site Details

* Site: Default

Step 3: Give IPEngine Camera Configuration Details

Camera Server and Video Details

* Camera Server: [Dropdown]

* Video Clip Directory: [Text Box]

* Video Format: PAL

Step 4: Add Selected Cameras to IPEngine

Add

Close

2. Select the check box corresponding to the camera or cameras that you want to add.
3. From the Site drop-down list, select the required site.
4. In the Camera Server drop-down list, select the MAXPRO NVR Camera Server.
5. In the Video Clip Directory box, type a path to store video clips.
6. In the Video Format drop-down list, select a format for the video.
7. Click Add.

Associating Partitions to the Recorder

You can associate partitions to recorder. Associating a partition to a recorder restricts a non-associated user of the partition from viewing the recorder or changing the settings of the recorder.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partition to a recorder

1. Click the Configurator tab.
2. Expand Devices in the navigation area.
3. Click the Recorders branch. The Recorders screen appears in the display area.
4. Double-click the recorder you want to associate. The General Settings screen appears.
5. Click the Partitions tab. The screen displays the associated partitions, if any.

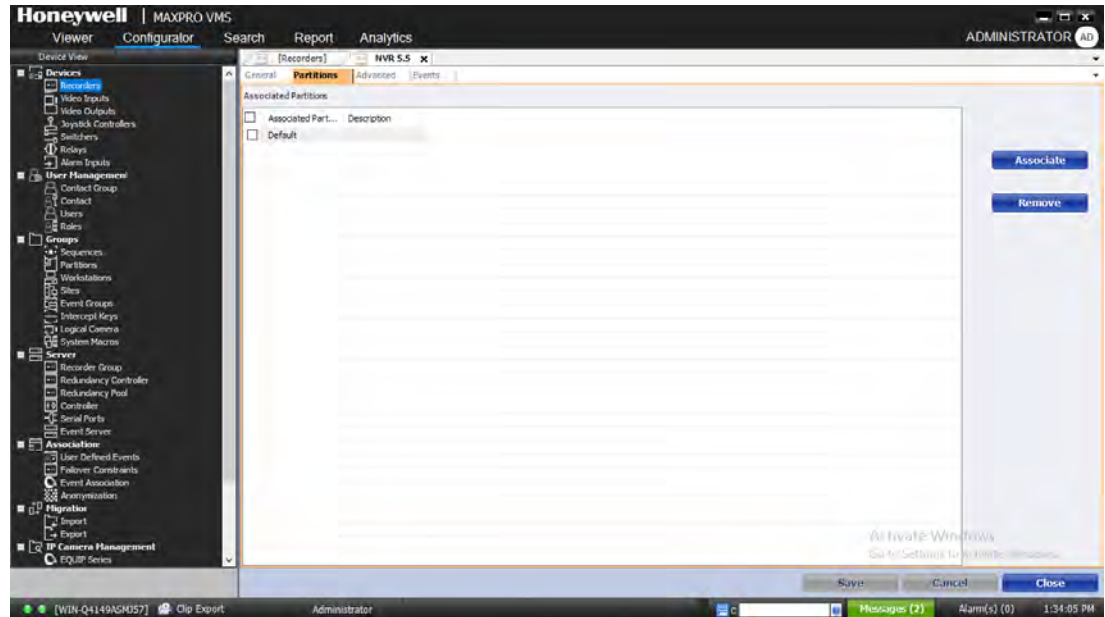


Figure 4-5 Recorder Partitions

6. Click Associate. The Select Partitions page appears.

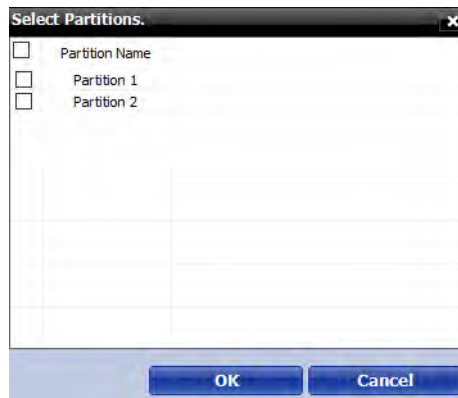


Figure 4-6 Select Partitions

7. Select the check box corresponding to the partition name you want to associate.
8. Click OK. The recorder is associated with the partition.

To disassociate partition from a recorder

- Select the check box corresponding to the partition name, and then click Remove.

Note: Partitions associated to a recorder cannot be removed unless they are removed from the devices that are connected to the same recorder.

Events

The following table explains the available events and their Severity Levels.

Event Name	Severity Level
MAXPRO NVR Server Connected	70
MAXPRO NVR Server Disconnected	70
Low Disk Space	70
Recording Server Connected	70
Recording Server Disconnected	70
MAXPRO NVR Controller Connected	70
MAXPRO NVR Controller Disconnected	70
Recorder Settings Retrieved	20
Recorder Manual Failover	70
Recorder Manual Failback	70
Recorder Automatic Failover	70
Recorder Automatic Failback	70
Low Archival Disk Space	70
Missing Archival Drive	50
Missing Storage Drive	50

Associating Events and Event Attributes to a Recorder

You can associate one or more events to a recorder. An alarm is triggered whenever any of the associated event occurs for the recorder. For certain events, you can also associate event attributes. For example, for an Encoder Disabled event, you can associate attributes such as Encoder Name, Encoder ID and so on. For every attribute that you associate, you can set a value based on which the event is triggered. In the above example, you can associate the attribute Encoder Name to the event and set its value as Encoder A. When this event is associated to the recorder, an alarm is raised when the event “Encoder Disabled” occurs for the Encoder Name “Encoder A”.

Attributes are available only for certain events. These events can be associated to a recorder multiple times. The event attributes are listed in the details of the alarm in Alarm window. To view the event attributes of an alarm, right-click the alarm, and then click Show Details.

After upgrading to R600, if user discovers the recorders then for only newly added recorders, by default all the events will not get associated to cameras. Only few events will be associated with the devices and cameras. If user need more events to be associated then it needs to be configured manually. See [Default Events Association](#) for more information.

To associate events to a recorder

1. Click the Events tab. The screen displays the associated events if any.

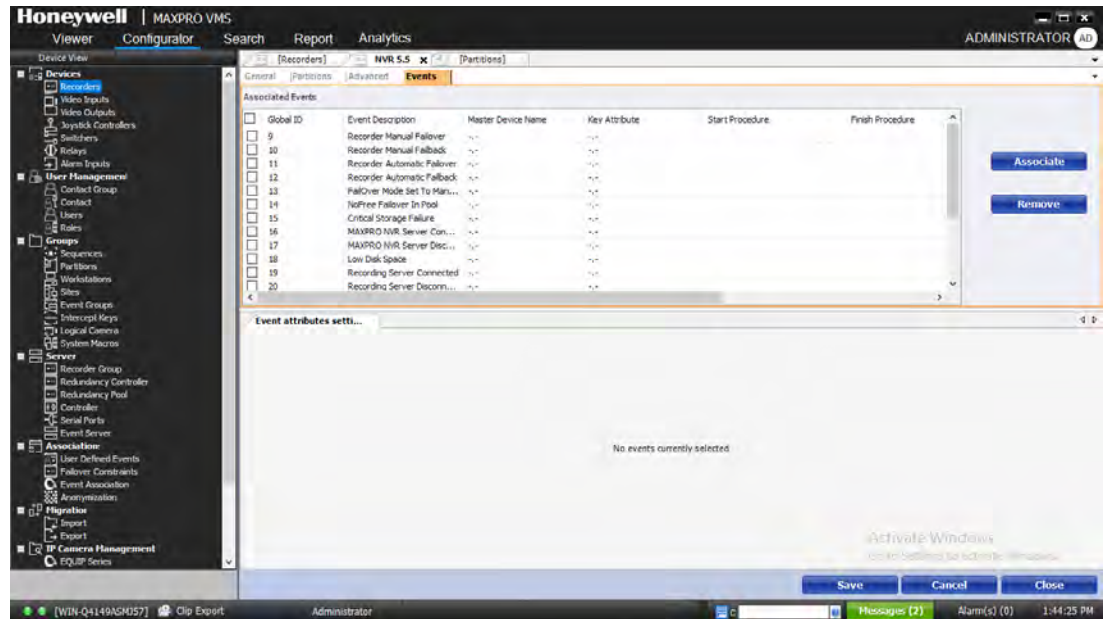


Figure 4-7 Recorder Events

2. Click Associate. The Select from List page appears.

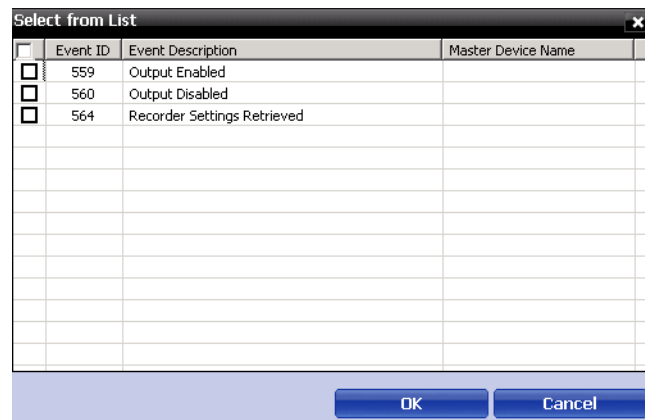


Figure 4-8 Select from List

1. Select the check box corresponding to the event you want assign severity level.
2. Click the value under the Severity Level column and edit the severity level.

Note: *Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.*

To enter remarks

1. Select the check box corresponding to the event you want to enter remarks.
2. Click the text under the Remarks column and type the remarks.

To assign macros

1. Select the check box corresponding to the event you want to assign macros.
2. Click the box under the Start Procedure column, and then type the required macro.
3. Click the box under the End Procedure column, and then type the required macro.

Associating Event Attributes

Before you begin

- Associate events.

To associate event attributes

1. Select the check box corresponding to the event for which you want to associate event attributes. The Event attributes Settings appear in the lower pane.
2. Click Associate. The Select Available Event Attributes page appears.
3. Select the check box corresponding to the event attributes that you want to associate.
4. Click OK.

To disassociate event attributes from a recorder

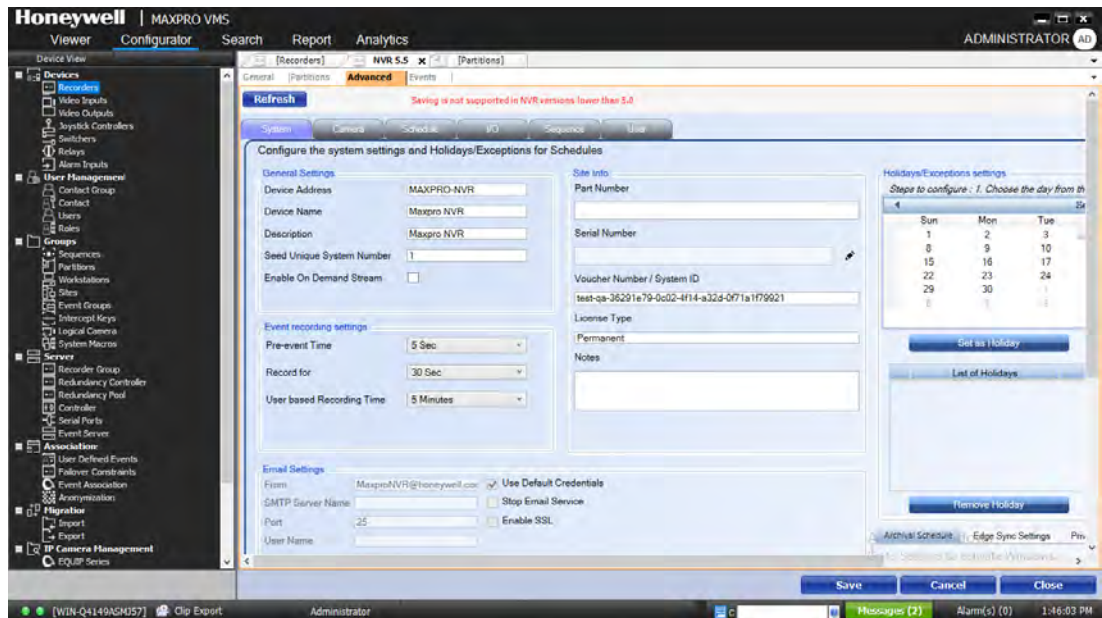
- Select the check box corresponding to the event attribute, and then click Remove.

The following table describes the recorder event name, event attributes, and their description.

Recorder	Event Name	Event Attributes	Attribute Description
MAXPRO VMS	MAXPRO VMS Sever Connected	Instance ID	Numeric value of the recorder ID
		VMS ID	Numeric value of the VMS ID
	MAXPRO VMS Server Disconnected	Instance ID	Numeric value of the recorder ID
		VMS ID	Numeric value of the VMS ID
	MAXPRO VMS Controller Connected	Instance ID	Numeric value of the recorder ID
		VMS ID	Numeric value of the VMS ID
	MAXPRO VMS Controller Disconnected	Instance ID	Numeric value of the recorder ID
		VMS ID	Numeric value of the VMS ID
MAXPRO NVR	Recording Server Connected		
	Recording Server Disconnected		
	Low Disk Space		
	Recording Server Connected		
	Recording Server Disconnected		
	MAXPRO NVR Controller Connected		
	MAXPRO NVR Controller Disconnected		
	Recording Settings Retrieved		

Advanced Settings

Caution: This tab displays only for the MAXPRO NVR recorder.



The configured settings for the MAXPRO NVR recorder are displayed in the following five tabs.

- System
- Camera
- Schedule
- I/O
- Sequence
- User

You can navigate to each of these tabs and change the configured settings as applicable.

Filtering and Grouping the Recorders

Filter feature enables you to filter and group the required number of recorder columns. Filtering recorders can be performed in two ways.

- By dragging and dropping specific column headers to group with the other columns.
- By defining the row values to display the required columns.

To filter and group the recorder columns by drag and drop

1. Click the Configurator tab.
2. Expand Devices in the navigation area.
3. Click the Recorders branch. The Recorders screen appears in the display area.

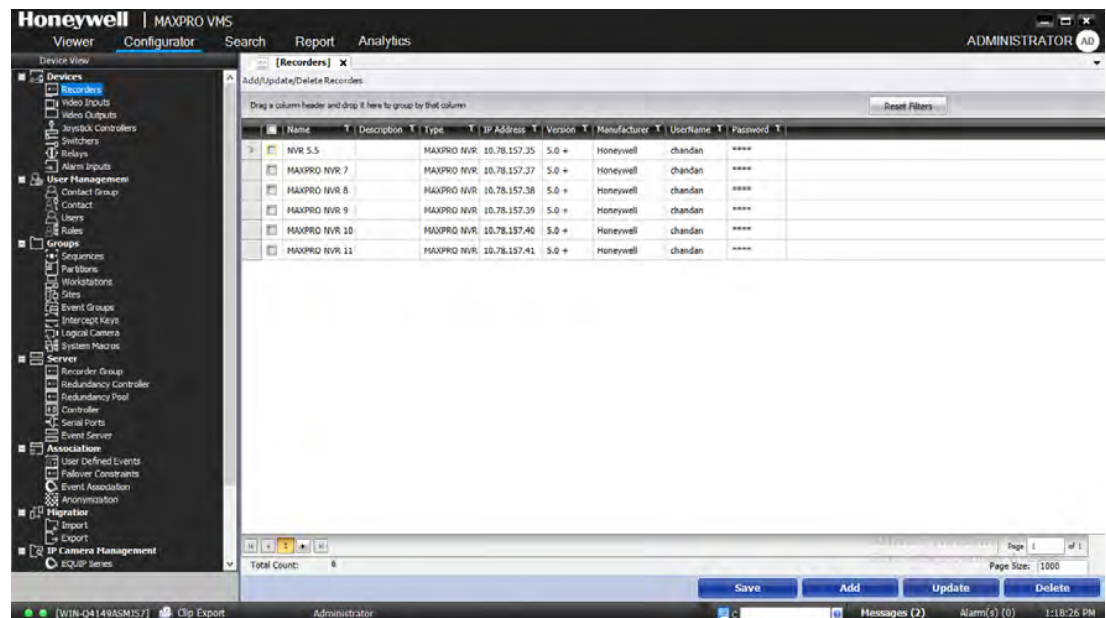


Figure 4-10 Recorder Filtering

4. Drag and drop the required columns in upper header area to view the corresponding column details.
Or
Right-click on the required column name and then choose Group by or Ungroup by option.
Example 1: If you want to view the details of only Name, Type and IP columns at once, drag and drop the columns one after another to the upper header area as shown below.

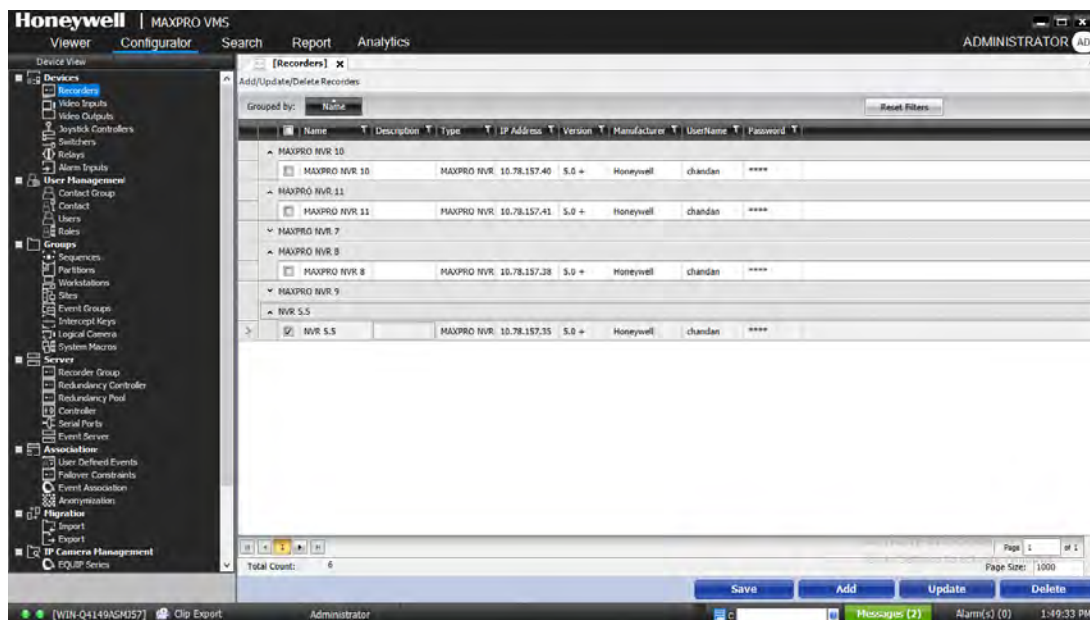
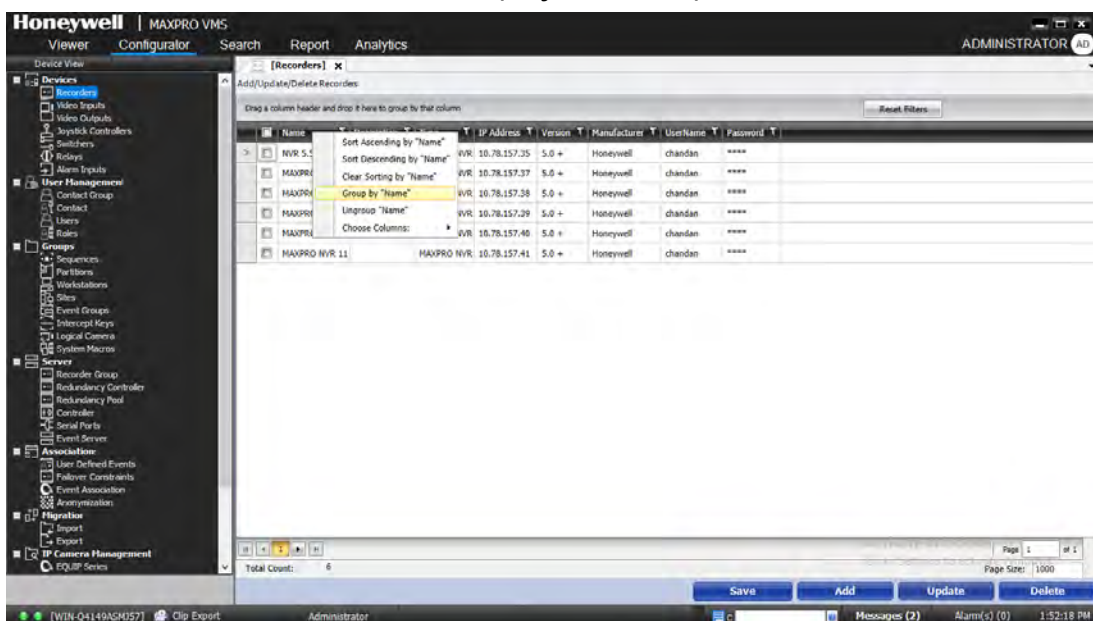
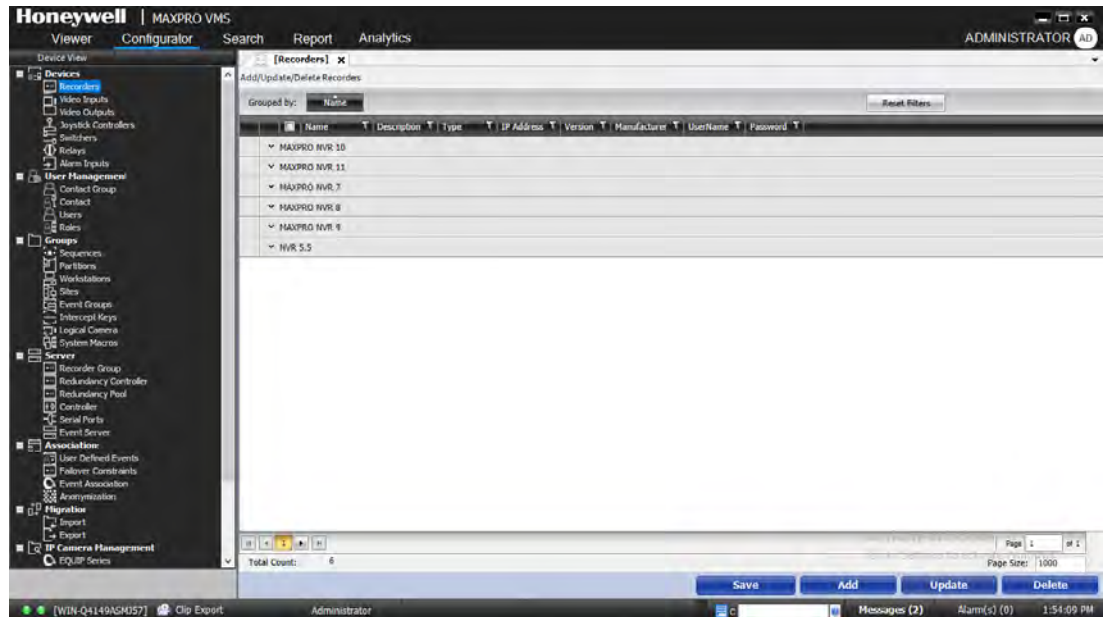



Figure 4-11 Recorder grouping

Example 2: If you want to group the columns by Name then right- click on the Name column and then choose Group by “Name” option as shown below.



The column arrangement is displayed a shown below.



5. Click  under each node to expand and view the details. Similarly repeat the step 4 to add more column headers.

To remove the column headers from the Grouped By area

- Drag the required columns from the Grouped By area and drop into the actual header area.

To filter the recorder columns by defining the value

1. Click the Configurator tab.
2. Expand Devices in the navigation area.
3. Click the Recorders branch. The Recorders screen appears in the display area.

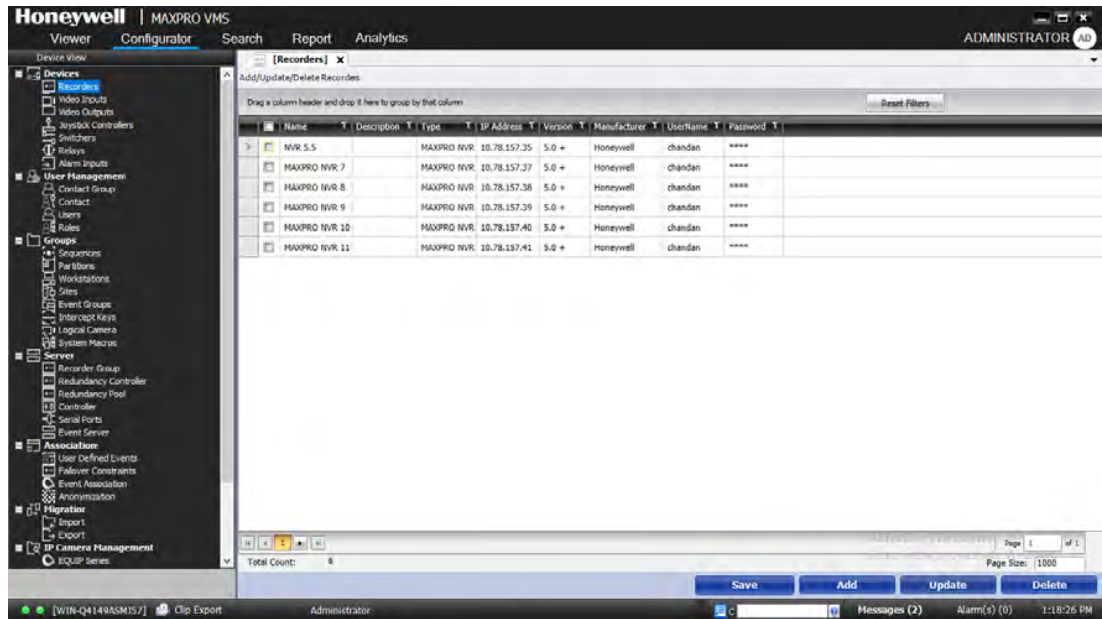

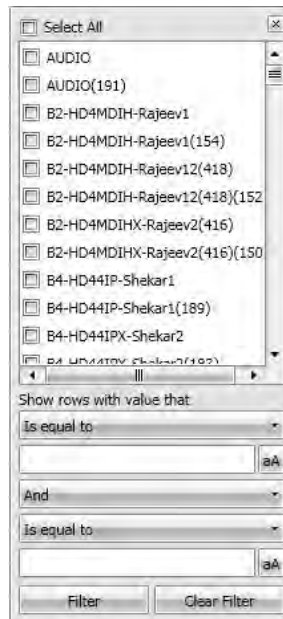
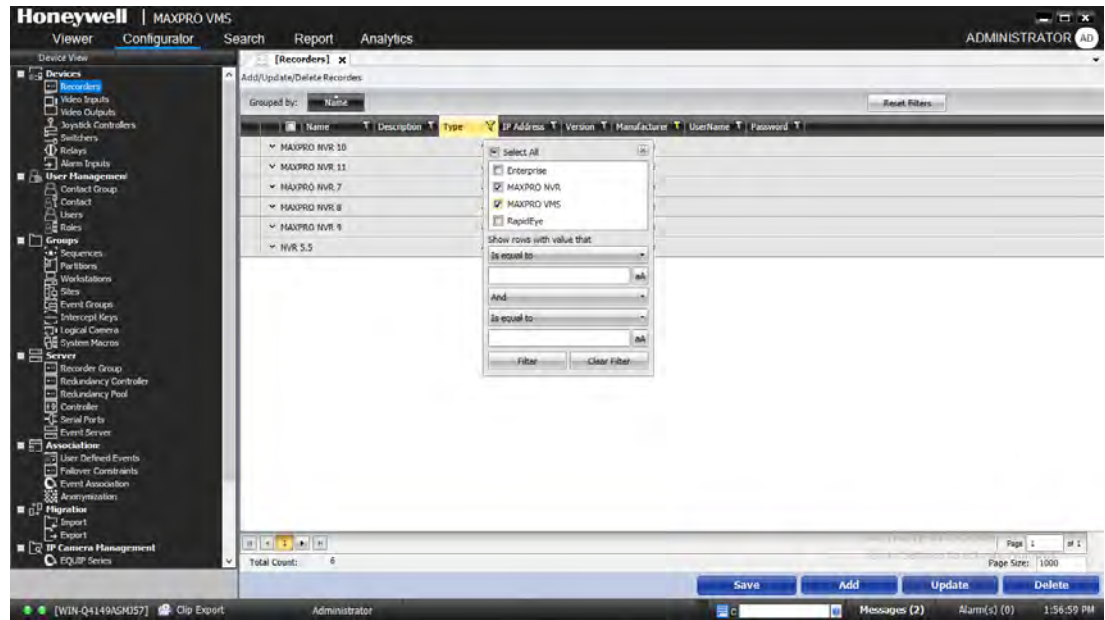


Figure 4-12 Recorder Screen

- Click  . Filter page is displayed as shown below.



5. Under Select All, select the required check boxes to display the row elements as shown below.



OR

In the Show rows with value that, perform the following:

- a. Select the required option from the Is equal to drop-down list.
- b. Type the required value corresponding to your selection.
- c. Select the required option from the AND/Or drop-down list.
- d. Select the required option from the Is equal to drop-down list corresponding to your option selected.
- e. Type the required value corresponding to your selections.
- f. Click Filter. The recorder columns based on your requirement is displayed. For example If you define a row value as:

value Starts with, MAXPRO NVR, And, that Is not equal to, ADPRO then the result of the filter is displayed as shown below.

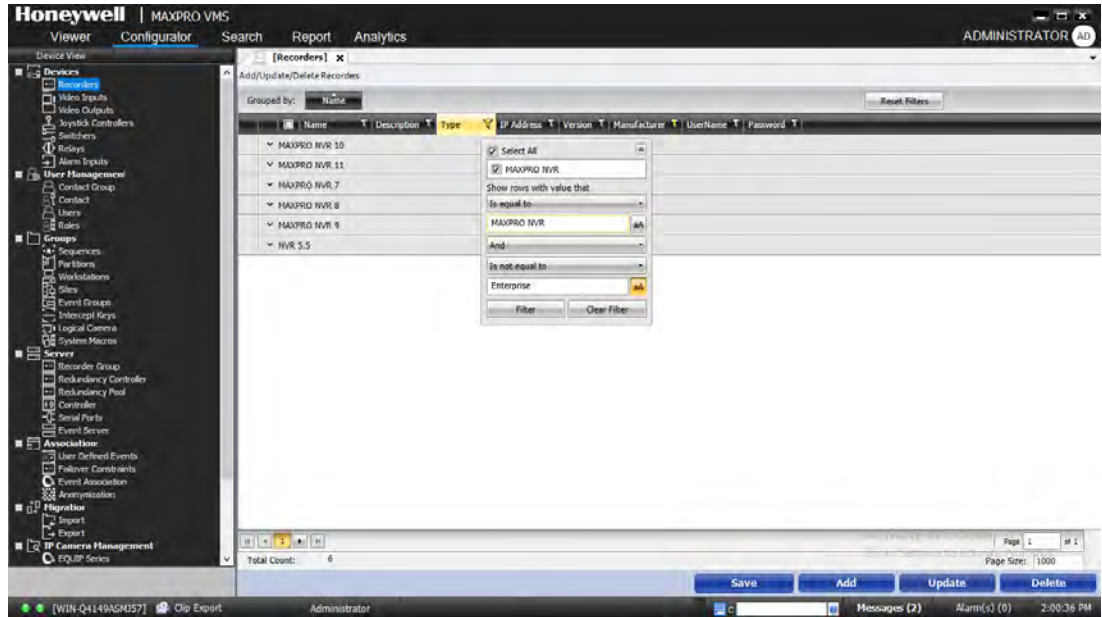


Figure 4-13 Defining Filter

To Clear or Reset the filter

- Click Clear Filter in the page
Or
Click the Reset Filter button to reset all the filters.

Sorting recorder

Sorting feature enables you to sort the required columns ascending or descending. It also allows you to group or ungroup based on the specific column.

To sort the columns ascending or descending

1. Click the Configurator tab.
2. Expand Devices in the navigation area.
3. Click the Recorders branch. The Recorders screen appears in the display area.

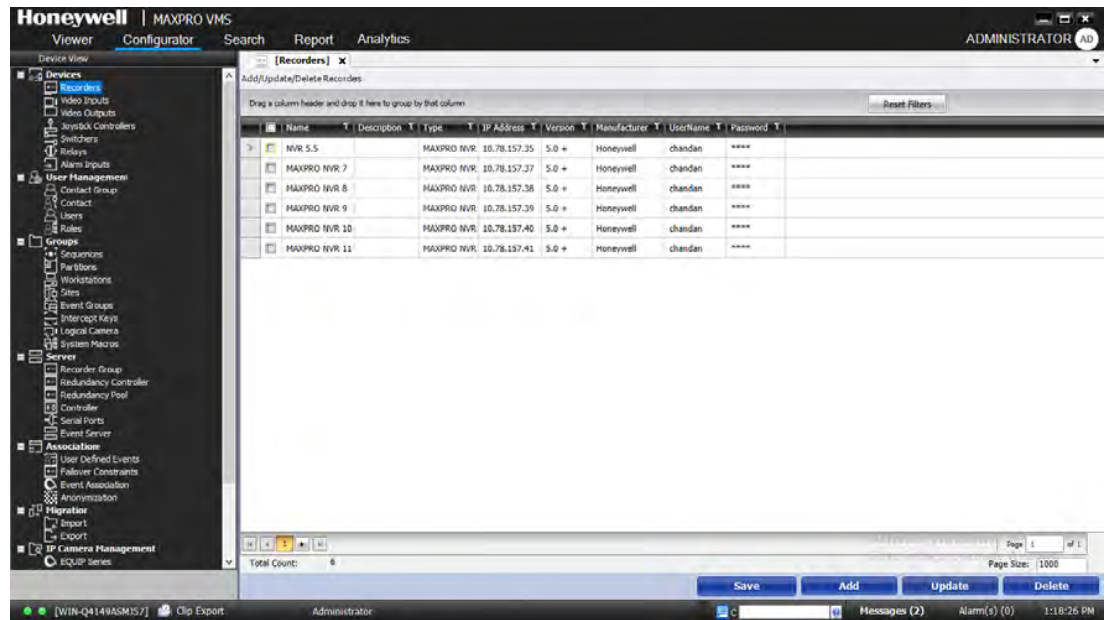
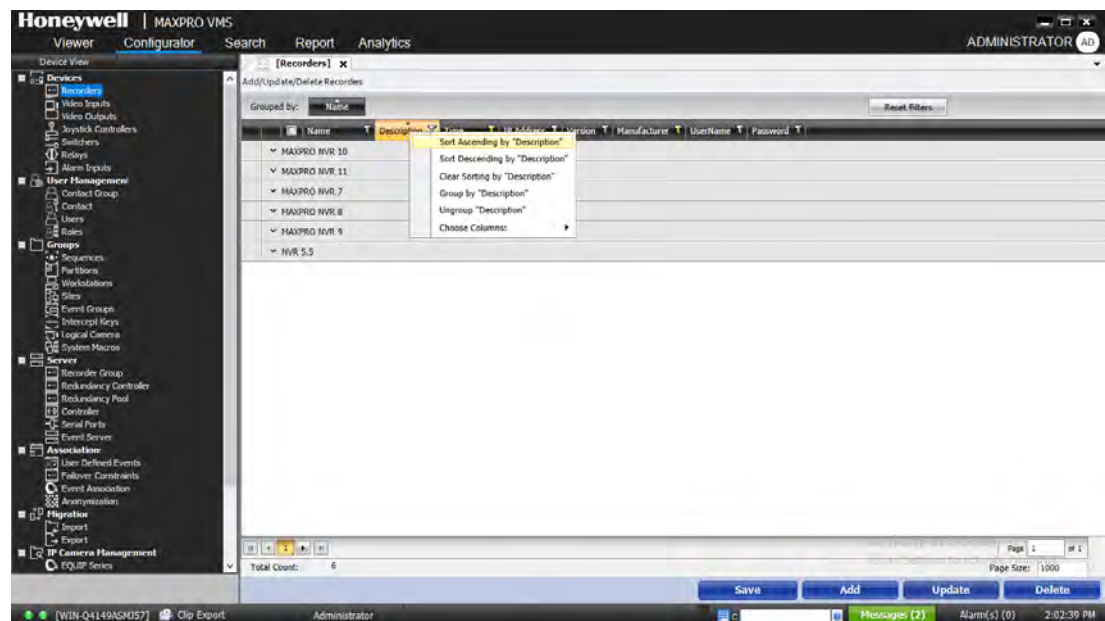


Figure 4-14 Recorder Screen

- Right click on the required column name. Sorting options are displayed as shown below.



- Choose the required Ascending or Descending option. The columns information is arranged accordingly as shown in [figure 11](#).

Choose the Columns to Display

You can choose the attributes of recorder to display in the recorders screen.

To choose the columns to display

1. Right click on any column header and then point to Choose Columns. The available column names are displayed.
2. Select or clear the required column. Based on the selection the column table are displayed.

Updating a Recorder

You can update a recorder to change the settings like the recorder name, site, site address, user ID, and password.

To update a recorder

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Recorders. The Recorders screen appears in the display area.
3. Select the check box corresponding to the recorder you want to update.
4. Click Update. The settings for the recorder appear. You can modify the settings.

Deleting a Recorder

Before you begin

Remove the associations with the video inputs or delete all the video inputs that are associated with the recorder.

To delete a recorder

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Recorders. The Recorders screen appears in the display area.
3. Select the check box corresponding to the recorder you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Video Inputs

Video inputs are devices through which video is supplied into MAXPRO VMS. Video input devices can be logically grouped in MAXPRO VMS so that selecting and updating them is easier.

The following types of video input devices are supported.

- Camera -fixed or PTZ.

- Standard Device - other devices, freeze frames, and so on.
- Smart Device - devices such as multiplexers.
- Trunk - trunk video input (from a networked system).
- VCR (Video Cassette Recorder)- dedicated or Dub VCR.
- Standby VCR - Standby VCR as used in VCR Management.
- Logging VCR - Monitor logging VCR as used in VCR Management.
- Menu - MAXPRO-Net system menu (using MaxMon).
- Black Source - black source for monitor blanking.
- Digital Input Trunk - to view analog camera video.

Video inputs and partitions

A partition is a logical grouping of video devices. Partitions are associated to cameras. You can restrict a non-associated user of the partition from viewing or changing the settings of the camera.

Video inputs and events

Events are predefined actions. Video inputs have events set by default. For example, when a camera connection is lost, an event 'CameraDisconnected' is generated. You can also associate event attributes to events. An alarm is triggered whenever an event is generated.

Video inputs and Analytics

Analytics can be configured for video inputs like cameras. Video analytics monitors the video from cameras at real time and triggers alarms to whenever an event occurs.

Adding Video Inputs

Before you begin

- Add Site. See [Adding a Site](#).
- Add Partition. See [Adding a Partition](#).
- Add Event Groups. See [Adding an Event Group](#).
- Add Recorders. See [Adding a Recorder](#).
- Add Switchers. See [Adding a Switcher](#).

By default, a site, partition, and event groups are available. You can associate the camera to them or create new.

You can add a camera to view live video and record video. You can associate cameras to partitions and events.

To add a video input

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Inputs. The Video Inputs screen appears in the display area, and displays the list of video inputs.

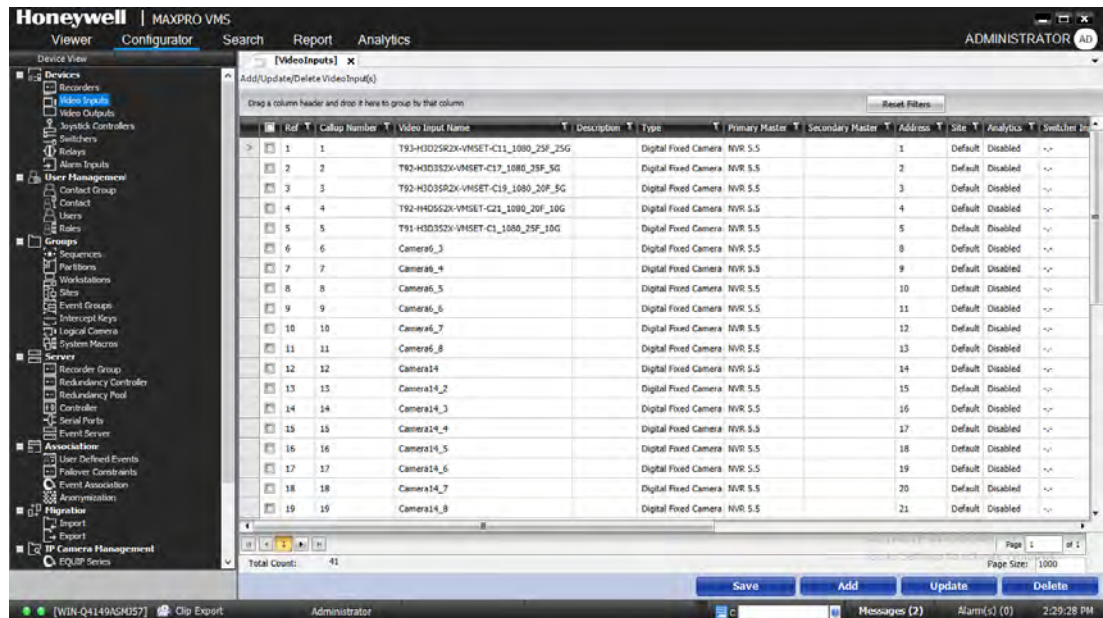


Figure 4-15 Video Inputs

3. Click Add. The General screen appears by default.

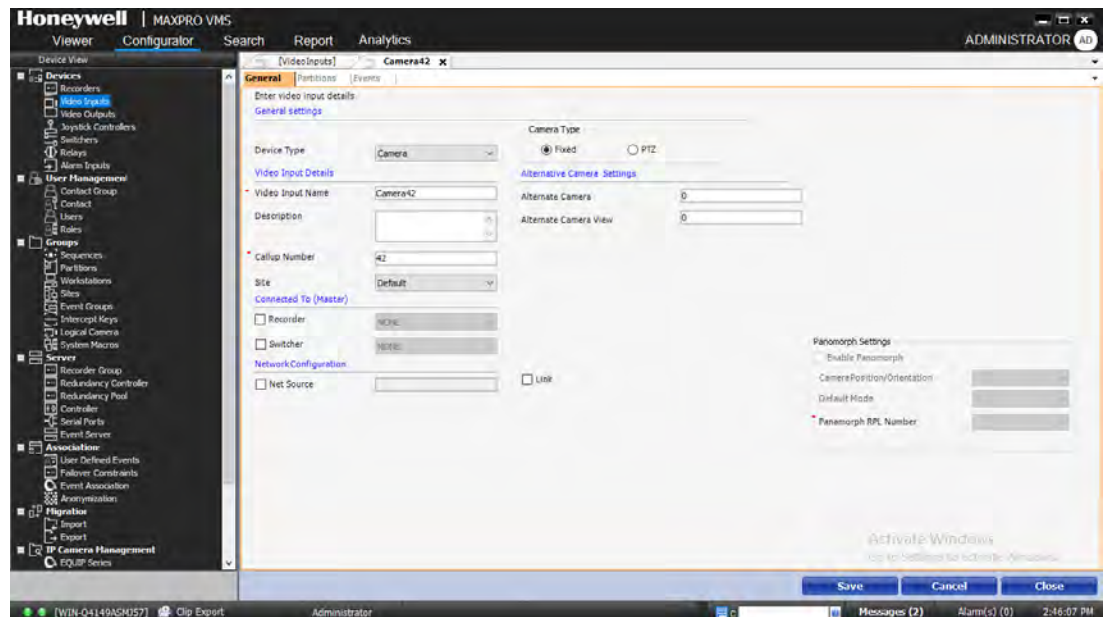


Figure 4-16 Camera Screen

4. From the Device Type drop-down list, select the required video input type. The currently supported video input device types are listed in the following table.

5. Associate Analytics. See [Associating Analytics](#) for more information.

Video Input Device	Description
Camera	For details on configuring a camera, see Adding a Camera .
Standard Device	For details on configuring the devices, see "Adding a Video Input Device" on page 5-167.
Smart Device	
Trunk	
VCR	
Standby VCR	
Logging VCR	
Menu	
Black Source	
Digital Input Trunk	For details on configuring a digital input trunk, see Adding a Video Input Device (Digital Input Trunk) .

Note: You can associate analytics only for cameras.

6. Associate Partition. See [Associating Partitions to Video Inputs](#) for more information.
7. Associate Events and Event Attributes. See [Associating Events and Event Attributes to a Video Input](#) for more information.
8. Click Save.

Adding a Camera

Adding a camera involves defining the camera's set up and operation across switchers and recorders. You can update or configure the general settings of a camera to configure PTZ settings and connect a camera to a recorder or switcher.

To configure a camera

1. In the Camera Type area, click PTZ Camera if the configured camera is PTZ or click Fixed Camera if the camera type is fixed.
2. In the Video Input Details area, specify the following camera details.

Field	Description
Video Input Name	Type a camera name. The camera name appears in the devices window making it easy to select.
Description	Type a description for the camera.

Field	Description
Callup Number	A unique number that identifies the camera. By default, the next available number is allocated. The operators can use the number to quickly view the live video from the camera using the virtual keyboard.
Site	Location of the camera.

3. In the Alternative Camera Settings area, specify the following details.

Settings	Description
Alternate Camera	Type the number of the camera that has to be selected alternate camera option is selected from the context menu while playing or viewing live video. The range of valid camera numbers is 1 – 999999999. Zero (0) is the default value and indicates no alternate camera is defined.
Alternate Camera View	Type the camera view number or preset number to select the preset view for the alternate camera. The valid camera views range is 1 – 99, 0 is the default value which indicates no camera view is to be selected.

4. In the Connected To (Master) area, select Recorder, if you want to connect the camera to a recorder (see [Associating Recorder to a Video Input Device](#) for more information). Select Switcher, if you want to connect the camera to a switcher (see [Associating a Switcher to a Video Input](#) for more information).

Note: If you select Recorder check box then Input Number (Recorder) text box is displayed. Type the input number for recorder.

5. Select the Net Source box when you want to view a video from a camera connected to the MAXPRO VMS within a network configuration. Specify the following details.




Settings	Description
Net Source	Specify the network node and the camera number from which you want the video input. When the current video input is actually connected to another MAXPRO VMS within a network configuration, the Net Source field is used to specify the exact location and reference for the video input device.
Link	Select if you want to broadcast the status changes and actions performed on the current video input device on the network.

Settings	Description
Switcher Settings, Advance Settings, and PTZ control Settings.	Configure the Switcher Settings and Advance Settings. See Associating a Switcher to a Video Input for more information. Configure the PTZ Control Settings. See Control Settings for more information.

6. Under Video Anonymization, select the required option from the Environment drop-down list to mask people in live video scene. The available options are:

Settings	Description
Variable Scene	Select this option if the scene contains both stationary and moving people or objects.
High Motion Scene	Select if you want to anonymize the objects in high motion scene
Still Scene	Select to anonymize the objects in a scene where the scene predominantly contains stationary people and objects.

To preview video when camera is associated to a recorder

- Select the Preview check box to view live video from the camera.
- Click the  icon to save the current image in the clip video directory.
- Click the  icon to open any saved image in the preview screen and position the camera accordingly.
- Click the  icon to delete the image in the preview screen.

Note: Using the preview option, a user can take snapshots of the area to be monitored by the surveillance camera and save them. These snapshots can be used to identify the proper location where the camera needs to be installed so that the desired field of view is obtained. This can also be used to reposition the camera and identify changes in camera field of view.

Associating Recorder to a Video Input Device

Video input devices like cameras and digital input trunk can be associated with different recorders. Video clips are recorded and stored in recorders.

To associate a camera to a recorder

1. In the Connected To section, select Recorder check box. The Recorder drop-down list is enabled.
2. Select the recorder. The device settings for the recorder appear. Perform the instructions listed in the following table.

Recorder Type	Instructions
MAXPRO NVR	Recorder Settings In the PTZ Sensitivity drop-down list, select a number for PTZ sensitivity.

Note: For more details on the camera specifications for other recorders, refer to the manuals that are provided along with the cameras.

Motion Detection Settings (Video Motion)

Configuring motion detection involves defining one or more Region of Interest (ROI) in the field of view. Rectangles or polygons are drawn in the field of view to specify the regions of interest, and then the motion detection algorithm is tuned within those regions.

Some of the considerations while configuring motion detection are:

- If the streamer supports streamer-based motion detection, use it to reduce the load on the computer.
- Motion detection recording and alarming is disabled while you are tuning motion detection (when you click Start Tuning).
- If you select the Premium algorithm, the algorithm uses the first 20 frames to learn the statistics of the field of view, and the next 60 frames to set up the information learned during the first 20 frames. Therefore motion is not detected in the field of view during the first 80 frames.

Before you begin

- Configure the camera settings. See [Adding a Camera](#) for more information.
- Associate the recorders. See [Associating Recorder to a Video Input Device](#) for more information.

To configure the motion detection

1. Click the Advance Settings tab by default the Record Settings tab appears.
2. Click the Video Analytics tab.
3. Select the Video Analytics enabled check box.
4. Use the General properties to set the algorithm, motion server, and detection type. The following table lists the General properties and the instructions to configure them.
5. Click Start tuning.

Settings	Description
Algorithm	Select Standard (Low CPU) or Premium (High CPU).
Motion Server	The Video Analytics Server you want to use to run the algorithm. (Only applicable to server-side algorithms.)
Detection Type	Select: Continuous - 24 hours a day, 7 days a week. Scheduled - the time(s) at which motion detection is enabled is specified in one or more schedules. See Schedules for more information. Note: Changing from Scheduled to Continuous deletes all video analytics schedules for the camera. The default is Continuous .

6. Use the ROI to define one or more regions. See [Defining Regions of Interest](#) for more information.
7. Use the tuning properties to set motion detection frame rate and sensitivity. Check if the algorithm is operating as required. (Tuning the algorithm's operation is typically an iterative task - you may have to change the values several times before you achieve satisfactory results.) See [Tuning Properties](#) for more information.
8. When satisfactory results are obtained, click Finish tuning.
9. Configure the When motion is detected properties as required. See [When Motion is Detected Properties](#) for more information.
10. Click Save.

Defining Regions of Interest

To define a rectangular region of interest

- Click and drag the pointer diagonally over the area that you want to track and classify objects. As you drag, a box marks the region of interest.

To define an irregular region of interest

1. Move the pointer to the location of the first vertex, and then click to mark its location.
2. Drag the mouse pointer to the place you want to add the next vertex and release the mouse button.
3. Click and drag the mouse pointer to the place you want to add the next vertex and release the mouse button.
4. Repeat step 3 for each of the other vertex, (you can have up to 10 vertices), except the last vertex.

5. Double-click to mark the last vertex or drag the mouse pointer to the first vertex of the shape and release the mouse button.

Note: To cancel the task of defining a region of interest, right-click or press the ESC key.

To select a region of interest

Click the region of interest to select it. (If regions of interest overlap, click the edge of the region to select.)

To modify a region of interest

1. Click the region of interest to select it. Selection handles appear.
2. Drag a selection handle as required. The vertices move as you drag.

To modify an irregular region of interest

1. Double-click at the point where you want to add a new vertex.
2. Drag the selection handle to create the new shape for region of interest.

To move a region of interest

1. Click the region of interest to select it.
2. Drag it to its new location.

Note: Dragging it by a selection handle might change its shape.

To delete a vertice

- Click the vertice and drag it onto the vertice next to it to merge them.

To delete a region of interest

1. Click the region of interest to select it.
2. Press DELETE.

Tuning Properties

Algorithm tuning properties involves configuring the motion detection by a camera depending on the frame rate of the motion, size of the object involved in motion and speed of the object involved in motion.

1. Click Start tuning, and then configure the settings for Standard (Low CPU) or Premium (High CPU) as per the algorithm you selected.

Standard (Low CPU) algorithm

The following table list the Standard (low CPU) algorithm tuning properties.

Premium (High CPU) Algorithm

The following table list the Premium (High CPU) algorithm tuning properties.

Settings	Description
Detection frame rate	<p>The frame rate you want the motion detection algorithm to detect a motion. (An object is considered to be “moving” if it moves inside a region of interest for at least two consecutive frames.)</p> <p>The chance of motion being detected depends on:</p> <p>The frame rate—a higher frame rate increases the chance of motion being detected.</p> <p>The size of the region of interest—the larger the region of interest, the longer the object takes to move through it, increasing the chance of motion being detected.</p> <p>The speed of the object—the faster the object moves the shorter is the amount of time required to pass through the region of interest, thereby decreasing the chance of motion being detected.</p> <p>The default frame rate is 3 frames per second. A higher frame rate increases the chance of a fast moving object being detected. The bandwidth at which the frames delivered is displayed.</p> <p>If you are using HNVE130A MPEG streams, VMD uses I-frames for video motion detection and the options available for this option are Every I-frame and Every second I-frame and so on.</p> <p>When you select this option, the frame rate given to the VMD algorithm is displayed.</p> <p>This setting has a high impact on the loading of the server (the higher the frame rate the higher the load on the CPU) and impacts the bandwidth used by the streamer when motion detection is activated.</p>
Optimize for movement	<p>(Applicable to the selected region of interest).</p> <p>Select the option you want to optimize the algorithm to detect the movement of any object.</p> <p>The options are:</p> <p>In any direction (the default)</p> <p>Across field of view</p> <p>To/from camera</p>
Sensitivity	<p>(Applicable to the selected region of interest).</p> <p>Indicates how sensitive the algorithm must be to detect movement. Values are between 1 and 100 and the higher the value the more sensitive to motion. The default is 40%.</p> <p>If the viewing resolution is changed, it affects this value.</p>

Settings	Description
Detection frame rate	<p>The detection frame rate description for Premium (High CPU) Algorithm is same as Standard (Low CPU) algorithm. See page 137.</p>
Sensitivity	<p>Specify whether the camera is aimed at an Indoors (High) or Outdoors (Low) scene. The default is Indoors (High).</p>

Settings	Description
Sub-sampling	<p>Reduces the effective resolution of the image used for detecting motion. The greater the level of sub-sampling, the lower the load on the CPU required for motion detection. The values are:</p> <p>1—no sub-sampling (the resolution of the image is not changed)</p> <p>2—the resolution of the image and the load on the CPU are halved</p> <p>4—the resolution of the image and the load on the CPU are quartered</p> <p>The default is 2.</p> <p>Increasing the sub-sampling might increase the chance of a false detection.</p>
Minimum object size	<p>Select the minimum size of an object for which motion can be detected, expressed in pixels.</p> <p>The minimum size you can specify is limited by the sub-sampling property, according to the following formula: $4 \times (\text{sub-sampling})^2$. For example, if you set sub-sampling to 2, the minimum object size you can specify is 16 pixels.</p> <p>The maximum object size is 64 pixels. If objects in the scene you want to detect motion are large, increasing the minimum object size can prevent false detections caused by small movement changes</p>

When Motion is Detected Properties

Specify the When Motion is Detected properties as follows:

Settings	Description
Consider motion finished after	<p>The length of time, after motion was last detected, that motion is considered to have stopped.</p> <p>This property affects When motion is detected properties as follows:</p> <p>A new alarm is not generated before this time has expired.</p> <p>A new recording does not start before this time has expired. If you set the Record for property to until motion finishes, recording continues until this time has expired.</p> <p>Video is not resent to a Station until this time has expired.</p> <p>If you have a lot of false detections occurring, increasing this value helps.</p> <p>If your motion detection recordings are configured to stop when the motion stops, and does not stop as anticipated, decreasing this value might help.</p>
Generate an alarm	<p>When checked, sends an alarm to the EBI, Experion, or HSS server at the specified Alarm level when motion is detected.</p> <p>The alarm is not latched to a point.</p>

Settings	Description
Alarm level	<p>The alarm level can be of type:</p> <p>Urgent</p> <p>High</p> <p>Low</p> <p>Journal (the default)</p> <p>All alarms, except Journal, appear in Station's Alarm Summary. Journal alarms do not appear in the Station Alarm Summary, but are written to the event file and appear in the Event Summary.</p> <p>Ensure that all operators who are required to view these alarms have access to the EBI, Experion, or HSS system area in which the alarms are being raised. This area is the same as the camera's configured area.</p>
Start a recording	Starts a recording when motion is detected. Selecting this allows you to specify Pre-record for, Record for, Record frame rate, and Archive after, and Delete after properties for video clips created when motion is detected.
Pre-record for	<p>The duration of video that the 600 recorder keeps in memory for motion detection recordings. When motion is detected and a recording is started, the IP engine inserts this pre-record segment at the start of the recording.</p> <p>Configuring a pre-record period on the recording allows you to view what was happening immediately before the motion was detected and a recording started. For example, if you set this to 10 seconds, the recording shows the 10 seconds of video before the recording was activated.</p>
Record for	The length of time (in seconds) recording takes place after motion is detected. If you select Until motion finishes, the recording continues until no motion is detected in the scene for the length of time specified in the Consider motion finished after property.
Record frame rate	The frame rate at which video is recorded for motion detection recordings.
Archive after	The period for which a motion detection recording is available for playback before being archived. The duration commences at the video clip's end date and time.
Delete after	The duration for which motion detection recordings are stored before being automatically deleted. The duration commences at the clip's end date and time.
Send video to station	If selected, video is automatically shown in the specified Station(s) when motion is detected. If a Station has an alarm monitor, the video is displayed on the alarm monitor.
Station number	The number of the Station that the video is sent to, if you select the Send video to Station(s) check box.
All stations in area	The area containing the Stations that the video is sent to, if you select the Send video to Station(s) check box.

Object Tracking and Classification Settings

Configuring object tracking and classification involves defining one or more Regions of Interest (ROI) - rectangles or polygons in the field of view, and then tuning the operation of the associated tracking algorithm within those regions.

In addition to defining the ROI, you must define:

- The minimum size of the object to be tracked.
- The condition that an object must meet for each region of interest before the network recorder takes the specified action—such as raising an alarm or starting a recording.

Before you begin

- Configure the camera settings. See [Adding a Camera](#) for more information.
- Associate the recorders. See [Associating Recorder to a Video Input Device](#) for more information.

To configure object tracking and classification

1. Click the Advance Settings tab. The Record Settings appears.
2. Click the Video Analytics tab.
3. Select the Video Analytics enabled check box.
4. Use the General properties to set the algorithm, motion server, and detection type. The following table lists the General properties and the instructions to configure them.

Settings	Description
Algorithm	Select Standard (Low CPU) or Premium (High CPU).
Motion Server	The Video Analytics Server you want to use to run the algorithm. (Only applicable to server-side algorithms.)
Detection Type	Select: Continuous - 24 hours a day, 7 days a week. Scheduled - the time(s) at which motion detection is enabled is specified in one or more schedules. See Schedules for more information. Note: Changing from Scheduled to Continuous deletes all video analytics schedules for the camera. The default is Continuous .

5. Click Start tuning.
6. Use the regions of interest to define one or more regions. See [Defining Regions of Interest](#) for more information.

7. Define the Minimum size of an object that is to be tracked. See [Defining the Minimum Object Size](#) for more information.
8. Use the tuning properties to set motion detection frame rate and sensitivity. See [Tuning Properties for Object Tracking](#) for more information.
9. Click Finish tuning if the tuning properties are satisfactory.
10. Configure the conditions for current ROI that moving objects must meet for each region of interest. See [Defining Conditions](#) for more information.

Defining the Minimum Object Size

The minimum object size that is tracked by the algorithm is defined by a magenta rectangle.

Note: *The position of the rectangle is not relevant for defining the minimum object size.*

To define the minimum object size

1. Select the rectangle. Its selection handles appear.
2. Drag a selection handle until the rectangle is of the required size and shape.

Tuning Properties for Object Tracking

Settings	Description
Detection frame rate	<p>The rate at which you want the algorithm to run. The default is 5 frames per second.</p> <p>This setting has a high impact on the loading of the server. The higher the frame rate, the higher the load on the CPU. It impacts the bandwidth used by the streamer when object tracking is activated.</p> <p>The chance of motion being detected depends on:</p> <p>The frame rate—a higher frame rate increases the chance of motion being detected.</p> <p>The size of the region of interest—the larger the region of interest, the longer the object takes to move through it, increasing the chance of motion being detected.</p> <p>The speed of the object—the faster the object moves the shorter is the amount of time required to pass through the region of interest, thereby decreasing the chance of motion being detected.</p> <p>If you are using HNVE130A MPEG streamers, AVPS uses I-frames for video motion detection and the options available for this option are Every I-frame and Every second I-frame and so on. When you select this option, the frame rate given to the AVPS algorithm is displayed.</p>
Sensitivity	Indicates whether the scene is indoor or outdoor.
Shadow correction	<p>If there are many shadows in the scene, turn shadow correction on, to reduce the risk of false detections.</p> <p>Turning this setting on, has a high impact on the loading of the server.</p>
Processing Type	<p>Indicates whether the algorithm analyzes the entire image (Full Frame) or only the regions of interest drawn (ROI Only).</p> <p>Full Frame processing provides more accurate results—especially for small regions of interest—because it can track objects over the whole frame. The larger the area in which the object might move and the longer it takes to move in the area, the camera has to classify more information and the detection is more accurate. However, it does increase the load on the CPU.</p> <p>Even if you select Full Frame, the conditions (and associated responses, such as raising alarms) only apply if the object enters a region of interest.</p>

Defining Conditions

You can define the condition or conditions that the moving objects must meet for each region of interest.

To define a condition

1. In the Region Name box, type the name of the region.
2. Click New. A condition row is added to list.
3. Define the condition by selecting appropriate values for the three condition properties: Object type, Behavior and Direction. The following table lists the settings to define the condition.

Note: As you select a value for each property, the condition in the list is updated.

Settings	Description
Object type	<p>The type of object you want the algorithm to detect. Valid types are:</p> <ul style="list-style-type: none"> • person • vehicle • other Object • any Object <p>When any Object is selected, it detects any moving object greater than the minimum object size.</p> <p>You cannot select Object type when using the object tracking algorithm. It is available only when using the object tracking and classification algorithm.</p>
Behavior	<p>The object's behavior that triggers the event. Valid behaviors are:</p> <p>Enter—enters the region</p> <p>Exit—exits the region</p> <p>Any behavior—matches any behavior</p> <p>Start and stop are only applicable if the Processing type property is set to Full Frame.</p>
Direction	<p>The direction in which the object must move to trigger the event (the exact wording depends on whether you set behavior to enter or exit):</p> <ul style="list-style-type: none"> • to/from the Right • to/from the Left • to/from the Bottom • to/from the Top • any Direction <p>Direction is with respect to the field of view—not the ROI, which may have an irregular shape.</p>

4. Configure the settings to define what should happen when an object satisfies the condition. The following table lists the settings and their description.

Settings	Description
Generate an alarm	Sends an alarm to the EBI, Experion, or HSS server at the specified Alarm level when an object satisfies the condition. The alarm is not latched to a point.
Alarm level.	The level of the alarms that are generated: <ul style="list-style-type: none"> • Urgent • High • Low Journal (the default) All alarms, except for Journal, appear in Station's Alarm Summary. Journal alarms does not appear in the Station Alarm Summary, but are written to the event file and appear in the Event Summary. Ensure that all operators who are required to view these alarms have access to the EBI, Experion, or HSS system area in which the alarms are being raised.
Start a recording	Selecting this allows you to specify Pre-record for, Record for, Record frame rate, and Archive after and Delete after properties for video clips created when an object satisfies the condition.
Pre-record for	The duration of video that the IP engine keeps in memory for motion detection recordings. When motion is detected and a recording is started, the IP engine inserts this pre-record segment at the start of the recording. The pre-record period on the recording allows you to view what was happening immediately before the motion was detected and a recording started. For example if you set this to 10 seconds, the recording shows the 10 seconds of video before the recording was activated.
Record for	The length of time (in seconds), the recording takes place after motion is detected. If you select Until motion finishes, the recording continues until no motion is detected in the scene for the length of time specified in the Consider motion finished after property.
Record frame rate	The frame rate at which video is recorded for motion detection recordings.

Settings	Description
Archive after	The period for which a motion detection recording is available for playback before being archived. The duration commences at the video clip's end date and time. If set, this must be less than the Delete after period.
Delete after	The duration for which motion detection recordings are stored before being automatically deleted. The duration commences at the video clip's end date and time.
Send video to station(s)	If selected, video is automatically shown in the specified Station(s) when an object satisfies the condition. If a Station has an alarm monitor, the video is displayed on the alarm monitor.
Station number	The number of the Station that the video is sent to, if you select the Send video to Station(s) check box.
All stations in area	The area containing the Stations that the video is sent, if you select the Send video to Station(s) check box.
Do not raise repetitive events for the same object for	The length of time, after the object has moved outside the region of interest, new alarms, recordings and video streams to Station are reserved. This property affects the other properties in this table as follows: <ul style="list-style-type: none"> • A new alarm is not generated until this time has expired. • A new recording does not start until this time has expired. In addition, if you set the Record for property to While object in the region, recording continues until this time has expired. • Video is not re-sent to a Station until this time has expired.

Schedules

A schedule defines the date and times when recording and video analytics (motion detection, and object tracking and classification) functions are enabled for a camera. A recurring schedule is a schedule that occurs at regular intervals.

Creating a Schedule

You can create schedules for the camera to record video at recurring intervals and to enable camera to record motion detection and object tracking at a stipulated time.

To create a schedule

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Inputs. The Video Inputs screen appears in the display area.
3. Double-click the camera or select the camera, and then click Update. The general settings for the camera appear.
4. Click the Advance Settings tab.
5. Click the Schedules tab, and then click Create a new schedule.
6. Configure the Schedule Details according to your requirement.

The following table lists the settings for configuring a schedule.

Type	Settings
Type	The type of schedule: Recording—records video as specified in the schedule. Video Analytics—controls when video analytics is enabled for the camera.
Start End	The date and time at which the schedule starts and stops. To specify the time, click each unit (hour and minute) and type the appropriate value.
Note	Description or comments about the schedule.
Frame rate	(Only applies to Recording schedules.) The frame rate at which the video is recorded.
Archive after	(Only applies to Recording schedules.)The period for which scheduled recordings are available for playback before they are automatically archived. If set, this must be less than the Delete after period.
Delete after	(Only applies to Recording schedules.) The time the recording is stored before it is automatically deleted.
Recurrence Details	
Recurring	Select No, if you want only one recording. Otherwise, select how often you want the recording to take place: <ul style="list-style-type: none">• Daily• Weekly• Monthly

Type	Settings
End after	(Only applicable if you select recurring.) If you want to create a recurring schedule that never expires, you must consider using background recording. The number of days before the schedule expires.

7. Click OK. The schedule is created.

Note: Clicking Cancel terminates the configured schedule.

Deleting a Schedule

You can delete a schedule for the camera when you do not want to record video at recurring intervals and disable camera from recording motion detection and object tracking at a stipulated time.

To delete a schedule

1. Click the Configurator tab.
2. Expand Devices in the navigation area.
3. Click the Cameras branch.
4. The Cameras screen appears in the display area.
5. Double-click the camera or select the camera, and then click Update. The general settings for the camera appear.
6. Click the Advance Settings tab.
7. Click the Schedules tab.
8. Select the start day for the schedule in Schedules on. The schedules for that day appear in the list. Ensure that you are deleting the right schedule.
9. Select the schedule you want to delete from the list. The schedule's details appear.
10. Click Delete, and then click Yes in response to the confirmation prompt.

To delete a recurring schedule

1. Select the start day for the schedule in Schedules on. The schedules for that day appear in the list.
2. Select the schedule you want to delete from the list. The details of the schedule appear.
3. Click Delete only if you want to delete the schedule occurrence on that day. If you want to delete all occurrences of the schedule, click Delete all occurrences. (This button appears only when you select a recurring schedule.)

Associating a Switcher to a Video Input

Switchers are devices that route multiple video inputs to multiple video outputs. You can associate video input devices like analog cameras, smart device, VCRs, and so on to a switcher. You can also configure switcher parameters like switcher input number, macros, and slot number.

Configuring the Switcher Settings

1. In the Connected to section, click Switcher. The Switcher drop-down list is enabled.
2. Select the required switcher. The Switcher Settings appear.
3. In the Input Number box, type the video input number on the subrack.
4. In the Device Macro Flags section, select the required fields to set the macro flag to True. This field allows for definition of the default cold boot state of the macro flags for the current video input device. Click Select All to set all the macro flags to True.
5. Under Pretext Settings, in the Pretext SubrackID box, type the address of the subrack which contains the text insertion card. The valid range of subrack addresses is 1 - 799, a value of 0 indicates pretext is not used.
6. In the Pretext SlotNumber, type slot number within the pretext subrack where the text insertion card resides. The valid range of slot numbers is 1 - 32.
7. In the X and Y boxes, type the location of the camera text to be displayed on the monitor. Valid positions are 1-13.

Configuring Control Settings

- Configure the [Control Settings](#) for the switchers.

Configuring Advanced Settings for MaxPro and VideoBlox

1. Click the Advanced Settings tab. The Advanced Settings screen appears.

Note: In the Primary Subrack ID, the ID that is associated while adding a switcher is displayed by default.

2. In the ByPass Subrack ID box, type the address of the subrack which must be bypassed when selecting the current video input device.

Note: For VideoBlox subrack, the Bypass subrack ID value must be 1-16, depending on the input device number. For the first 1-255 physical inputs, the bypass ID is 1, and for the next 1-255 inputs, the bypass ID is 2, and so on.

3. In the Combiner Subrack ID box, type the ID for cascading and combining configurations. In a cascading configuration consisting of three subracks, the Combiner Subrack ID contains the address of the second subrack that is to be bypassed when selecting the current video input device. The valid address values range from 0 (signifying no cascading or combining are used) through 99.

4. In the Combiner Input Number box, type the address to which the preselector subrack for the current video input is connected.
5. In the Dynamic Equalization box, type the value between 1 and 8 to represent the cable length between the video input and the switcher. It serves to improve video quality by compensating for cable related transmission losses.

Note: The values 1 - 8 represent one hundred meters of RG-59/BU units coaxial cable.

6. In the Video Fail Slot box, type the slot number where the video fail detector module is located.

Note: The valid subrack slot numbers are 11 - 14. HD Series subracks (HMX32128) perform video fail detection on the HMX128 subrack controller card. This is mapped to pseudo slots as follows:

Video Input	Video Fail Slot
1 - 32	11
33-64	12
65-96	13
97-128	14

Note: For VideoBlox subrack, the Video fail slot must be 1. Enter 0, if video fail detection is not required.

7. In the Start Macro box, type the desired macro number to execute Start Macro, whenever a video alarm condition is detected for the corresponding video input device.
8. In the End Macro box, type the desired macro number. The End Macro is executed whenever the video alarm condition is cleared.

Control Settings

1. Select the Locked check box to prevent the user to control the device.
2. From the PTZ Done By drop-down list, select the required PTZ type.

The following table lists the PTZ types and steps to configure their settings.

Type	Settings
Device	This setting is used when the PTZ camera is controlled using the recorder. The PTZ settings are done using the local applications of the recorder.

Type	Settings
Serial Port	<p>The followings settings are used when a PTZ camera is controlled by MAXPIT or MATPIT.</p> <ol style="list-style-type: none"> In the Select Serial Port drop-down list, select the serial port. In the Source Control ID box, a default ID is displayed. In the Source Control Slot box, type the slot number within the control subrack where the controller for the current video input device resides. <p>Valid slot numbers are 1 – 32 for I/O and combination video/I/O subracks and 1 – 8 for HD Series subracks. Within subracks such as HMX1132 and HMX1600, the control slot is the physical slot where the controller card resides. Whereas within HD Series subracks (HMX32128) device control and I/O functions are mapped to pseudo slots as all of these functions exist on the subrack controller card (HMX128) located in slot 0. For VideoBloxsubrack, the control slot number should be greater than zero. Valid range: 1 to 4.</p> <ol style="list-style-type: none"> In the Offset box, type the ID number of the PTZ site receiver connected to that camera. <p>The valid range for site IDs is 1 – 16. A 0 indicates that a hardwired relay output module is being used in the subrack slot for controlling that camera. Offset is the hardware address configured in the PTZ camera.</p>
Switcher	<p>The followings settings are used when a PTZ camera is controlled by a matrix switcher.</p> <ol style="list-style-type: none"> In the Select Switcher drop-down list, select the switcher. In the Source Control ID box, a default ID is displayed. <p>The valid range for Control ID is 1 – 799, a value of 0 indicates no control capability for the device.</p> <ol style="list-style-type: none"> In the Source Control Slot box, type the slot number within the control subrack where the controller for the current video input device resides. <p>Valid slot numbers are 1 – 32 for I/O and combination video/I/O subracks and 1 – 8 for HD Series subracks. Within subracks such as HMX1132 and HMX1600, the control slot is the physical slot where the controller card resides. Whereas within HD Series subracks (HMX32128) device control and I/O functions are mapped to pseudo slots as all of these functions exist on the subrack controller card (HMX128) located in slot 0. For VideoBlox subrack, the control slot number should be greater than zero. Valid range: 1 to 4.</p> <ol style="list-style-type: none"> In the Offset box, type the ID number of the PTZ site receiver connected to that camera. <p>The valid range for site IDs is 1 – 16. A 0 indicates that a hardwired relay output module is being used in the subrack slot for controlling that camera. Offset is the hardware address configured in the PTZ camera.</p>

5. In the PTZ Viewer Sensitivity drop-down list, select the required sensitiveness.
6. In the Available Control Options area, select the options to enable or disable the control functions. The available control functions vary between the different types of video input device as shown in the following figures.

The following tables lists the available control functions for different types of video input devices.

Camera	VCR or LoggingVCR or Standby VCR	Standard Device or Smart Device
Wash/Wipe	Record	Output1
Manual Iris	Play	Output2
Pan	Rewind	Output3
Tilt	Fast Forward	Output4
Focus	Slow	Output5
Zoom	Pause	Output6
Present View	Eject	Output7
Ext/Walk/Flashback	Stop	Output8

Associating Events and Event Attributes to a Video Input

You can associate one or more events to a video input. An alarm is triggered whenever any of the associated event occurs for the video input. For certain events, you can also associate event attributes. For example, for an Encoder Disabled event, you can associate attributes such as Encoder Name, Encoder ID and so on. For every attribute that you associate, you can set a value based on which the event is triggered. In the above example, you can associate the attribute Encoder Name to the event and set its value as Encoder A. When this event is associated to the video input, an alarm is raised when the event “Encoder Disabled” occurs for the Encoder Name “Encoder A”.

Attributes are available only for certain events. These events can be associated to a video input multiple times. The event attributes are listed in the details of the alarm in Alarm window. To view the event attributes of an alarm, right-click the alarm, and then click Show Details.

Before you begin

- Add a Video Input

Associating Events

To associate events to video inputs

1. Click the Events tab. The screen displays the associated events if any.

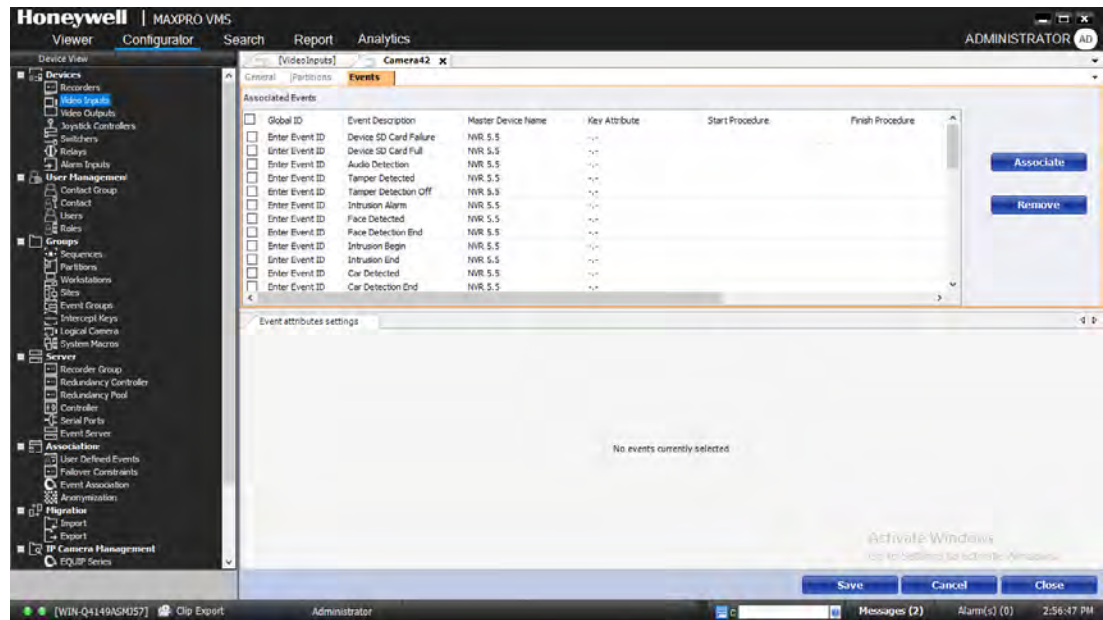


Figure 4-17 Camera Events

2. Click Associate. The Select from List page appears.

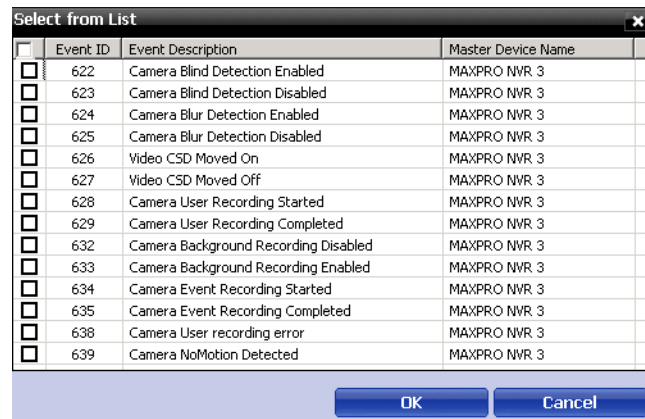


Figure 4-18 Select from List

3. Select the check box corresponding to the event you want to associate.
4. Click OK.

To disassociate events to video input

- Select the check box corresponding to the event, and then click Remove.

To add Event Groups to events

1. Select the check box corresponding to the event for which you want to add the Event Group.
2. Double-click the cell under the Event Group column. Select EventGroup page appears.

3. Click the check box corresponding to the Event Group you want to add.
4. Click OK.

Note: You need to add an event group before you associates it to an event. See [Adding an Event Group](#) for more information.

To disable an event

1. Select the check box corresponding to the event you want to disable.
2. Click the cell under the Disabled column. A drop-down list is enabled.
3. Select True.

To assign severity level

1. Select the check box corresponding to the event you want to assign the severity level.
2. Click the cell under the Severity Level column and edit the severity level.

Note: Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

To enter remarks

1. Select the check box corresponding to the event you want to enter remarks.
2. Click the cell under the Remarks column and type the remarks.

To assign macros

1. Select the check box corresponding to the event you want to assign macros.
2. Click the cell under the Start Procedure column, and then type the required macro.
3. Click the cell under the End Procedure column, and then type the required macro.

Associating Event Attributes

Before you begin

- Associate events.

To associate event attributes

1. Select the check box corresponding to the event for which you want to associate event attributes. The Event attributes Settings appear in the lower pane.
2. Click Associate. The Select Available Event Attributes page appears.
3. Select the check box corresponding to the event attributes that you want to associate.

4. Click OK.

To disassociate event attributes from a video input

- Select the check box corresponding to the event attribute, and then click Remove.

The following tables describes the event name, event attributes, and their description related to cameras with analytics.

Events	Event Attributes	Attribute Description
Video lost in analytics server	Server name	Server name
Video restored in analytics server	Server name	Server name
Camera Blind Detected	Camera blind	Camera blind in percentage
Camera Blur Detected	Camera blur	Camera blur in percentage
Scene changed	Scene changed	Scene changed in percentage
Car counted in lane	Object count	Car count
Car entered restricted zone	Zone information	Zone information
Car exited restricted zone	Zone information	Zone information
Car parked in handicapped zone	Zone information	Zone information
Entered target zone	Object type	Object type
	Zone information	Zone information
Object entered restricted zone	Object type	Object type
	Zone information	Zone information
Person counted as entering	Object count	Object count
	Zone information	Zone information
	Object type	Object type
Person counted as exiting	Object count	Object count
	Zone information	Zone information
	Object type	Object type
Person entered restricted zone	Zone information	Zone information

Events	Event Attributes	Attribute Description
Person exited restricted zone	Zone information	Zone information
Person loitering in restricted zone	Zone information	Zone information
Staying in target zone	Object type	Object type
	Zone information	Zone information
Object trespassing line	Object type	Object type
	Zone information	Zone information
Person trespassing line	Zone information	Zone information
Car trespassing line	Zone information	Zone information
Object started moving in wrong direction	Object type	Object type
	Zone information	Zone information
Object stopped moving in wrong direction	Object type	Object type
	Zone information	Zone information
Person started moving in wrong direction	Zone information	Zone information
Person stopped moving in wrong direction	Zone information	Zone information
Car started moving in wrong direction	Zone information	Zone information
Person on fence line	Zone information	Zone information
Car made an illegal U-turn	Zone information	Zone information
Car pulled off the road	Zone information	Zone information
Person running in the wrong direction	Zone information	Zone information
Person started running	Zone information	Zone information
Person stopped running	Zone information	Zone information
Car needs assistance	Zone information	Zone information

Events	Event Attributes	Attribute Description
Object entered	Object type	Object type
	Zone information	Zone information
Object exited	Object type	Object type
	Zone information	Zone information
Object stopped	Object type	Object type
	Zone information	Zone information
Object started moving	Object type	Object type
	Zone information	Zone information
Object merged	Object type	Object type
	Zone information	Zone information
Objects split	Object type	Object type
	Zone information	Zone information
People passed by	Object type	Object type
	Zone information	Zone information
Object entered sterile zone	Object type	Object type
	Zone information	Zone information
Car entered sterile zone	Zone information	Zone information
Person entered sterile zone	Zone information	Zone information

Associating Partitions to Video Inputs

You can associate partition to cameras. Associating a partition to a camera restricts a non- associated user of the partition from viewing the camera or changing the settings of the camera.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partitions to video inputs

1. Click the Partitions tab. The screen displays the associated partitions, if any.

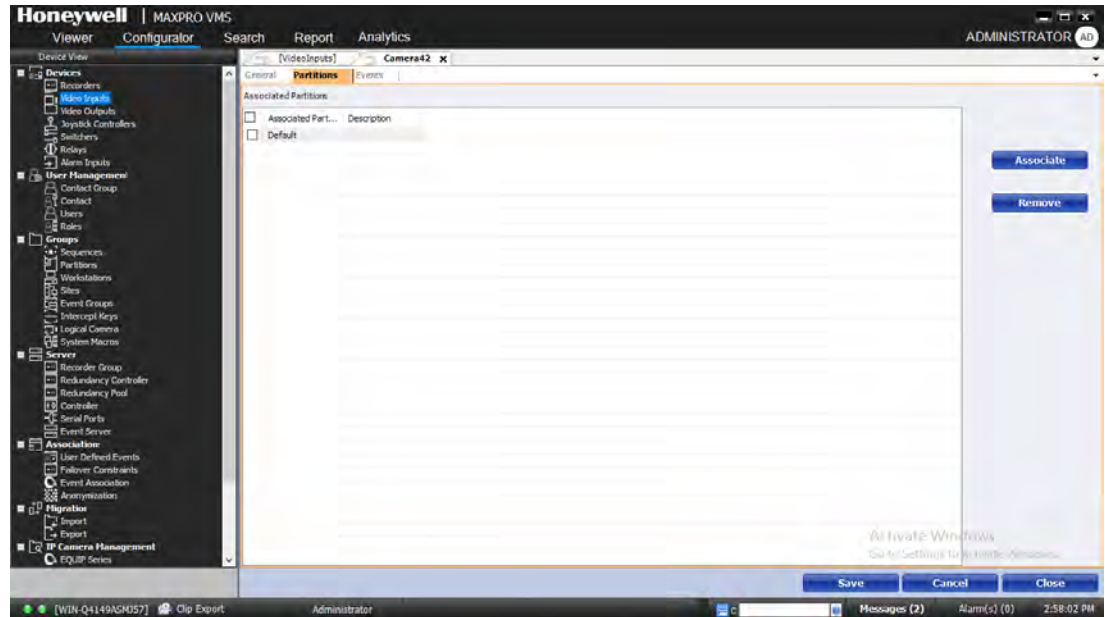


Figure 4-19 Camera Partitions

2. Click Associate. The Select Partitions page appears.
 3. Select the check box corresponding to the partition name you want to associate.
 4. Click OK. The selected partition is displayed in the list of associated partitions.
- To disassociate partitions to camera
- Select the check box corresponding to the partition name, and then click Remove.

Associating Analytics

Before you begin

Add Analytics Server. See [Adding an Analytics Server](#) for more information.

To associate analytics

1. Click the Analytics tab.

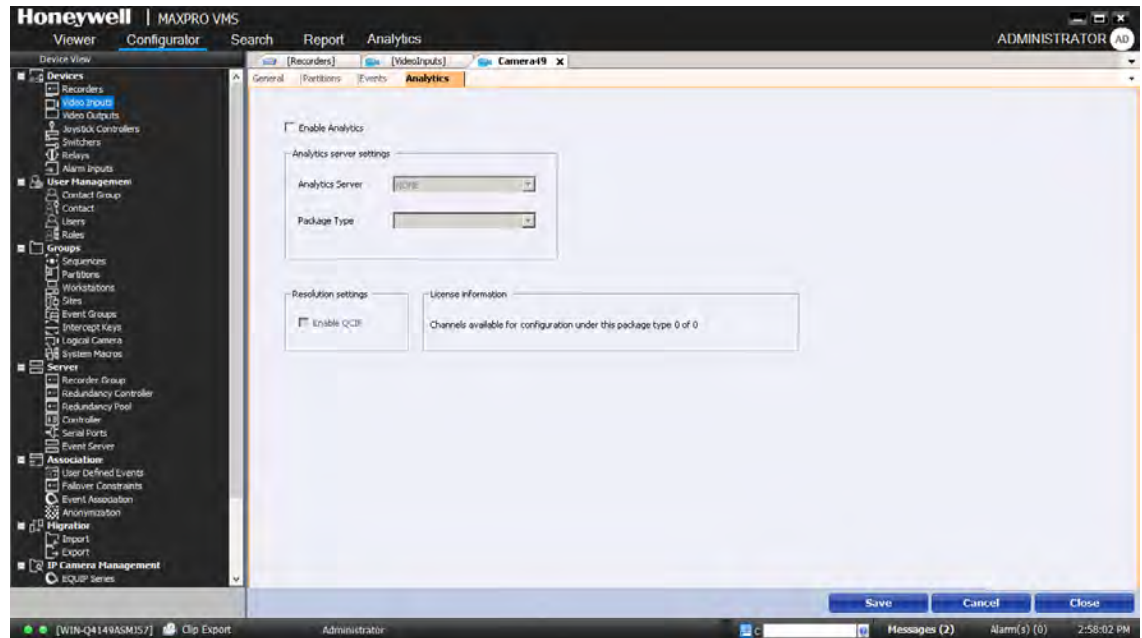


Figure 4-20 Camera Analytics

2. Select Enable Analytics.
3. From the Analytics Server drop-down list, select the required analytics server.
4. From the Package Type drop-down list, select the required package data.
5. In the resolution settings, select Enable QCIF to set the QCIF resolution if required.
6. Click Save.

Filtering and Grouping the VideoInput(s)

Filter feature enables you to filter and group the required number of video input columns. Filtering video inputs can be performed in two ways.

- a. By dragging and dropping specific column headers to group with the other columns.
- b. By defining the row values to display the required columns.

To filter and group the video input(s) columns

1. Click the Configurator tab.
2. Expand Devices in the navigation area.
3. Click the VideoInput(s) node. The VideoInput(s) screen appears in the display area.

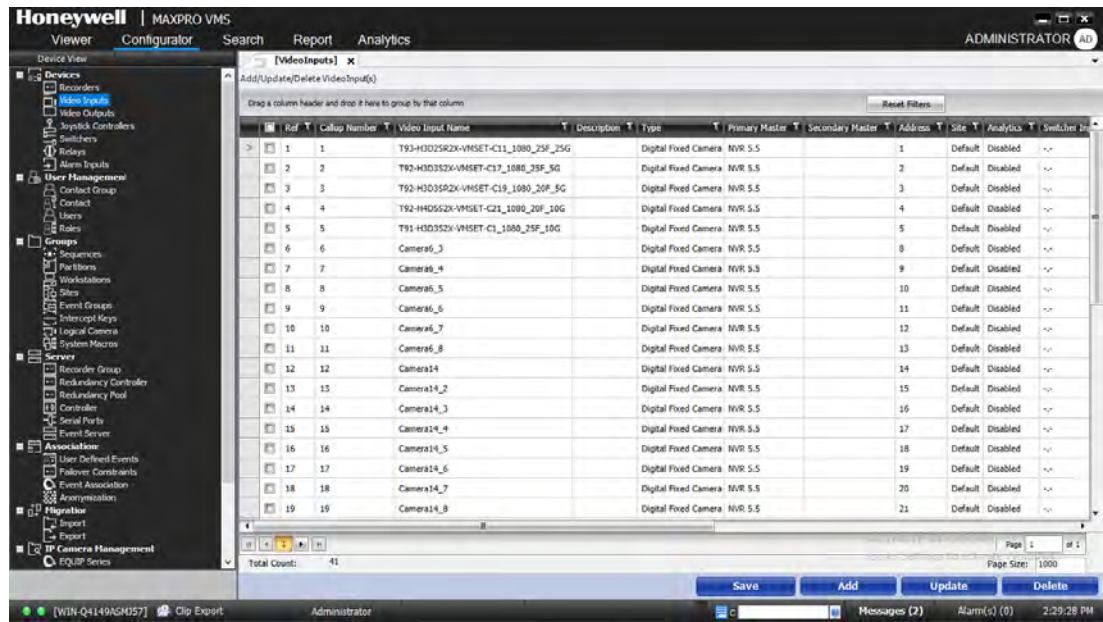


Figure 4-21 Video Inputs Filtering

4. Drag and drop the required columns in upper header area to view the corresponding column details.
 Or
 Right-click on the required column name and then choose Group by or Ungroup by option.
 Example 1: If you want to view the details of only VideoInputName, Type and Address at once, drag and drop the columns one after another to the upper header area as shown below.

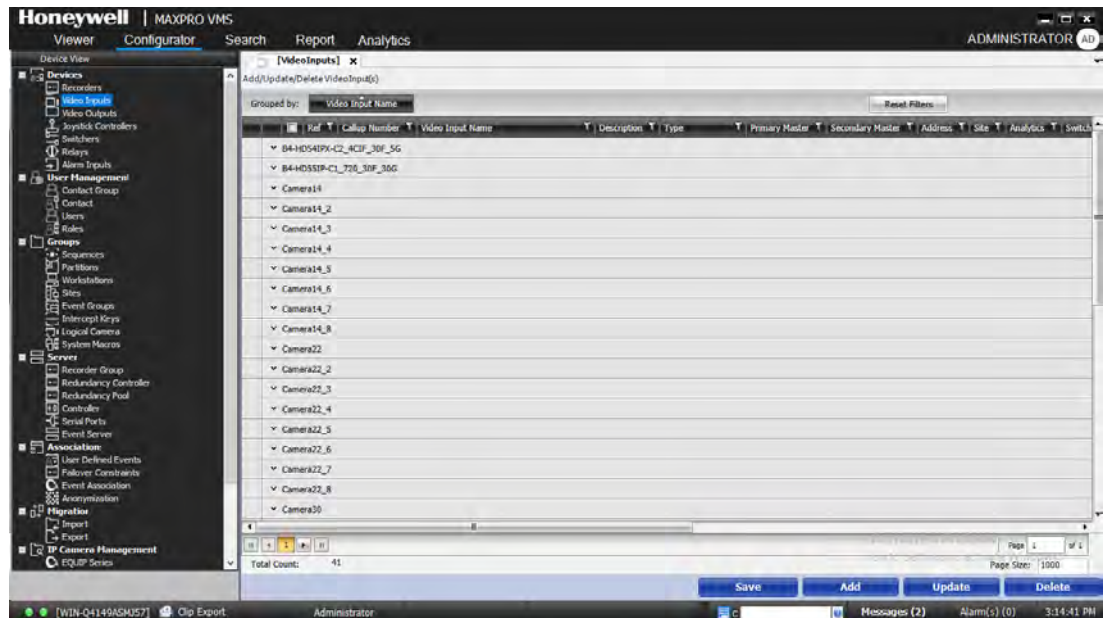
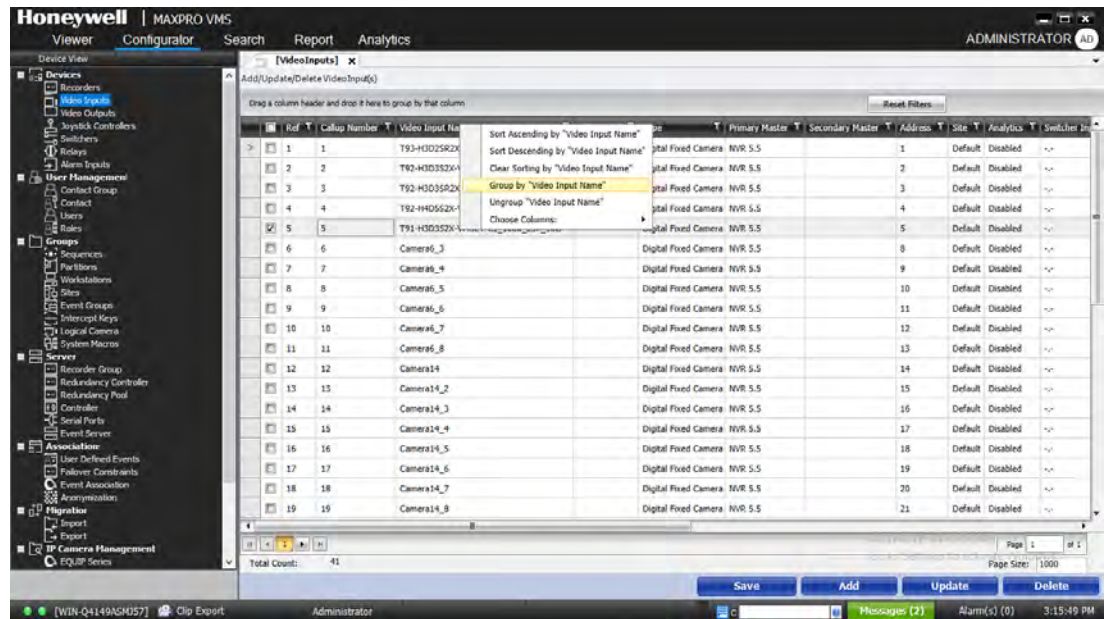
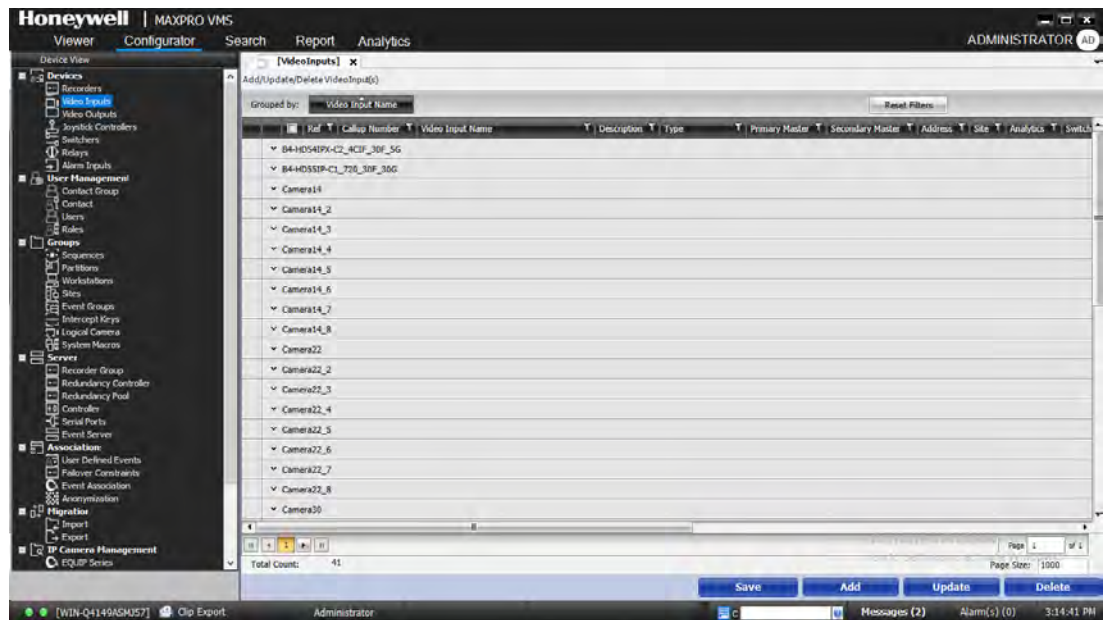



Figure 4-22 Video Inputs Grouping

Example 2: If you want to group the columns by VideoInputName then right- click on the Name column and then choose Group by “VideoInputName” option as shown below.



The column arrangement is displayed a shown below.



- Click  under each node to expand and view the details. Similarly repeat the step 4 to add more column headers.

To remove the column headers from the Grouped By area

- Drag the required columns from the Grouped By area and drop into the actual header area.

To filter the video inputs(s) columns by defining the value

1. Click the Configurator tab.
2. Expand Devices in the navigation area.
3. Click the Video Inputs(s) node. The Video Inputs(s) screen appears in the display area.

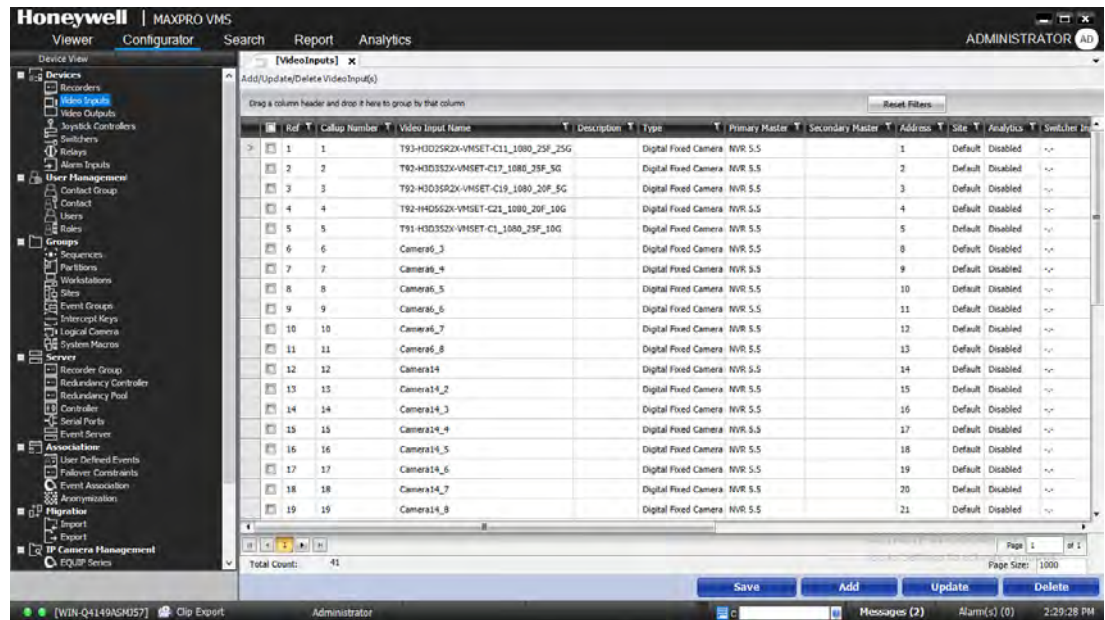

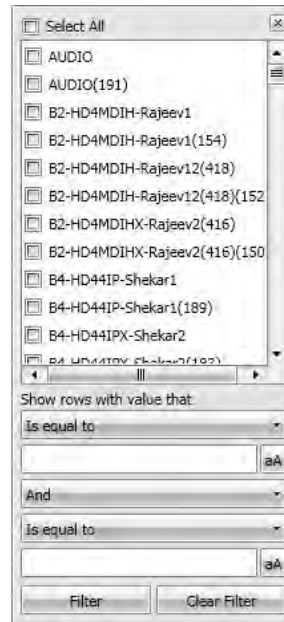


Figure 4-23 Video Inputs(s) Screen

4. Click  . Filter page is displayed as shown below.



The filter dialog box contains a list of video inputs under the 'Select All' section. The list includes:

- AUDIO
- AUDIO(191)
- B2-HD4MDIH-Rajeev1
- B2-HD4MDIH-Rajeev1(154)
- B2-HD4MDIH-Rajeev12(418)
- B2-HD4MDIH-Rajeev12(418)(152)
- B2-HD4MDIH-Rajeev2(416)
- B2-HD4MDIH-Rajeev2(416)(150)
- B4-HD44IP-Shekar1
- B4-HD44IP-Shekar1(189)
- B4-HD44IP-Shekar2
- B4-HD44IP-Shekar2(189)

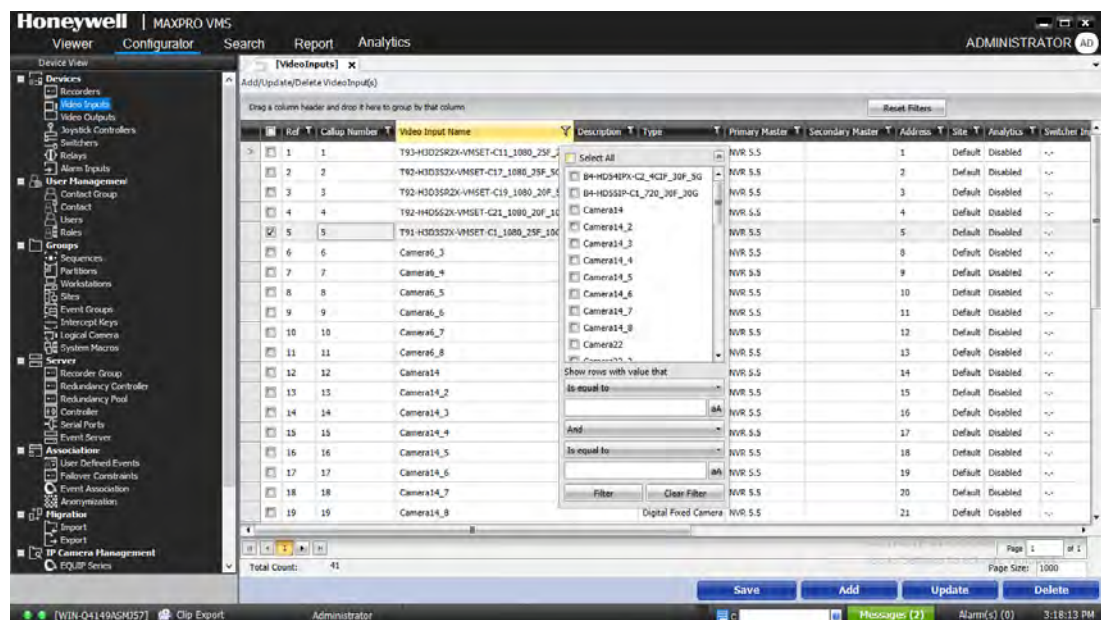
Below the list, there are two filter criteria sections:

Show rows with value that
Is equal to
[] [aA]

And
Is equal to
[] [aA]

Buttons: Filter, Clear Filter

5. Under Select All, select the required check boxes to display the row elements as shown below.



The screenshot shows the Honeywell MAXPRO VMS interface. The 'Filter' dialog box is open, and the 'Select All' section is checked. The table below shows the filtered results:

Id	Calup Number	Video Input Name	Description	Type	Primary Master	Secondary Master	Address	Site	Analytics	Switcher
1	1	T93-HD02SR2X-VHSET-C11_1080_25F_1	[] Select All	NVR 5.5			1	Default	Disabled	--
2	2	T92-HD03SR2X-VHSET-C17_1080_25F_54	[] B4-HD44IP-C2_4CIF_30F_30	NVR 5.5		2	Default	Disabled	--	
3	3	T92-HD03SR2X-VHSET-C19_1080_25F_4	[] B4-HD03SR-C1_720_30F_30G	NVR 5.5		3	Default	Disabled	--	
4	4	T92-HD03SR2X-VHSET-C21_1080_25F_14	[] Camera14	NVR 5.5		4	Default	Disabled	--	
5	5	T91-HD03SR2X-VHSET-C1_1080_25F_104	[] Camera14_2	NVR 5.5		5	Default	Disabled	--	
6	6	Camera6_3	[] Camera14_3	NVR 5.5		6	Default	Disabled	--	
7	7	Camera6_4	[] Camera14_4	NVR 5.5		7	Default	Disabled	--	
8	8	Camera6_5	[] Camera14_5	NVR 5.5		8	Default	Disabled	--	
9	9	Camera6_6	[] Camera14_6	NVR 5.5		9	Default	Disabled	--	
10	10	Camera6_7	[] Camera14_7	NVR 5.5		10	Default	Disabled	--	
11	11	Camera6_8	[] Camera14_8	NVR 5.5		11	Default	Disabled	--	
12	12	Camera14	[] Camera22	NVR 5.5		12	Default	Disabled	--	
13	13	Camera14_2	[] Camera22_2	NVR 5.5		13	Default	Disabled	--	
14	14	Camera14_3	[] Camera22_3	NVR 5.5		14	Default	Disabled	--	
15	15	Camera14_4	[] Camera22_4	NVR 5.5		15	Default	Disabled	--	
16	16	Camera14_5	[] Camera22_5	NVR 5.5		16	Default	Disabled	--	
17	17	Camera14_6	[] Camera22_6	NVR 5.5		17	Default	Disabled	--	
18	18	Camera14_7	[] Camera22_7	NVR 5.5		18	Default	Disabled	--	
19	19	Camera14_8	[] Camera22_8	NVR 5.5		19	Default	Disabled	--	
20	20	Camera14_9	[] Camera22_9	NVR 5.5		20	Default	Disabled	--	
21	21	Camera14_10	[] Camera22_10	NVR 5.5		21	Default	Disabled	--	

Buttons: Save, Add, Update, Delete

OR
In the Show rows with value that, perform the following:

- Select the required option from the Is equal to drop-down list.
- Type the required value corresponding to your selection.
- Select the required option from the AND/Or drop-down list.

- d. Select the required option from the Is equal to drop-down list corresponding to your group option selected.
- e. Type the required value corresponding to your selections.
- f. Click Filter. The video input(s) columns based on your requirement is displayed. For example If you define a row value as: Value Start with B4 And that Contains H4D551P model camera then the result of the filter is displayed as shown below.

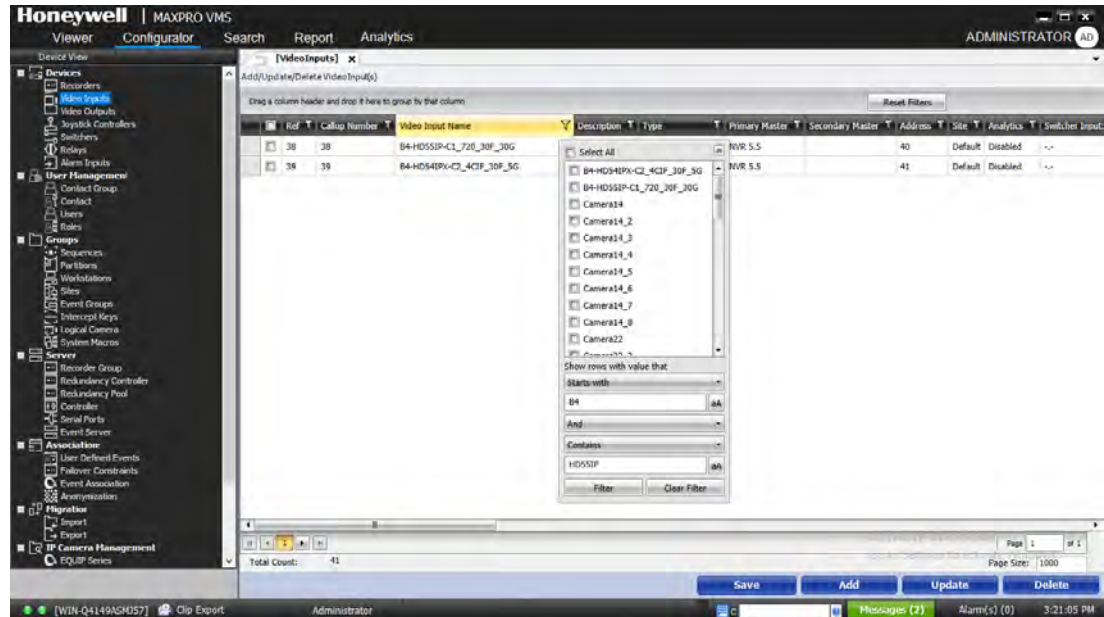


Figure 4-24 Defining Filter

To Clear or Reset the filter

- Click Clear Filter in the page
Or
Click Reset Filter to reset all the filters.

Sorting Video Input(s)

Sorting feature enables you to sort the required columns ascending or descending. It also allows you to group or ungroup based on the specific column.

To sort the columns ascending or descending

1. Click the Configurator tab.
2. Expand Devices in the navigation area.
3. Click the Video Input(s) branch. The Video Input(s) screen appears in the display area.

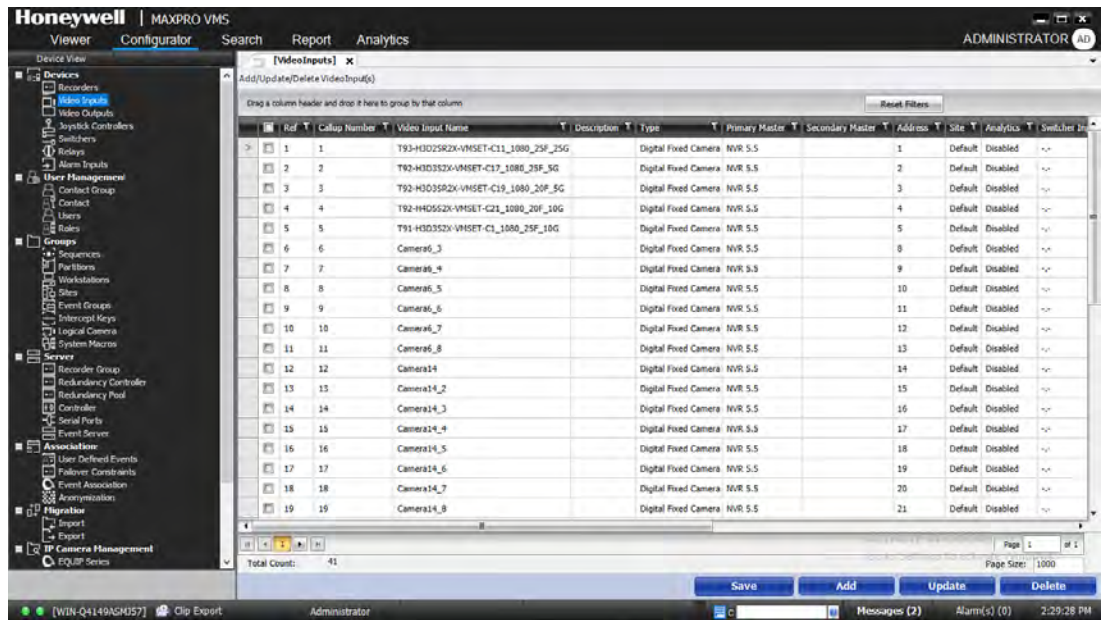
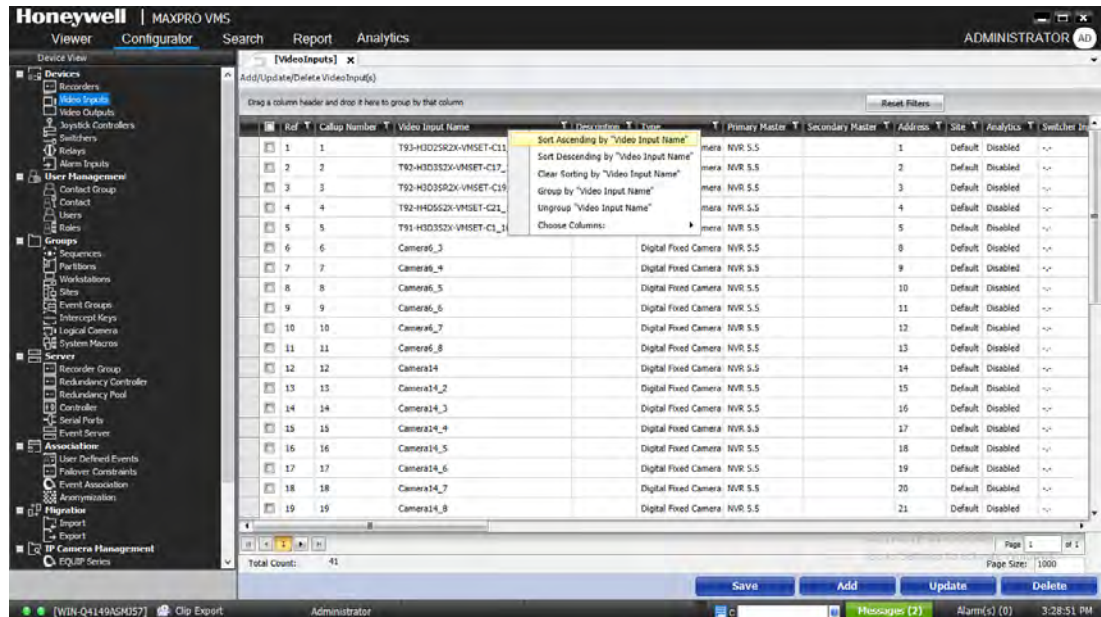


Figure 4-25 Video Input(s) Screen

- Right click on the required column name. Sorting options are displayed as shown below.



- Choose the required Ascending or Descending option. The columns information is arranged accordingly as shown in [figure 22](#).

Choose the Columns to Display

You can choose the attributes of video input(s) to display in the screen.

To choose the columns to display

1. Right click on any column header and then point to Choose Columns. The available column names are displayed.
2. Select or clear the required column. Based on the selection the column table are displayed.

Updating a Video Input

You can update the camera to change the existing settings and configure new settings.

To update a video input

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Inputs. The Video Inputs screen appears in the display area.
3. Double-click the video input or select the check box corresponding to the video input, and then click Update.
4. The Video Input screen appears. Update the required settings.
5. Click Save.

Deleting a Video Input

You can delete a video input when you do not want to record video from a site or do not want the display of a live video from a site. All the associations made to the video input are removed, when you delete it.

Before you begin

- Disassociate Partitions. See [Associating Partitions to Video Inputs](#) for more information.
- Disassociate Events. See [Associating Events](#) for more information.

To delete a video input

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Inputs. The Video Inputs screen appears in the display area.
3. Select the check box corresponding to the video input that you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Adding a Video Input Device

1. In the Video Input Details area, specify the following video input device details.
2. Repeat the step 2 through step 5 of section [Adding a Camera](#) on page 132
3. Click Save.

Adding a Video Input Device (Digital Input Trunk)

1. In the Video Input Details area, specify the following video input device details.

Field	Description
Video Input Name	Type a video input device name. The video input device name appears in the devices window making it easy to select.
Description	Type a description for the camera.
Callup Number	A unique number that identifies the camera. By default, the next available number is allocated. The operators can use the number to quickly view the video from the video input device using the virtual keyboard. See About Virtual Keyboard in Monitoring a Site section.
Site	Location of the camera.

2. In the Alternative Settings area, specify the following details.

Field	Description
Alternate Camera	Type the number of the camera that has to be selected as an alternate camera when ALT key is pressed on the keyboard. The range of valid camera numbers is 1 – 9999. Zero (0) is the default value and indicates no alternate camera is defined.
Alternate Camera View	Type the camera view number or preset number to select the preset view for the alternate camera. Pressing the 'ALT' key not only displays the alternate camera, but also move it automatically, to the designated VIEW preset. The valid camera views range is 1 – 99, 0 is the default value which indicates no camera view is to be selected.

3. In the Connected To section, select Switcher. See [Associating a Switcher to a Video Input](#) for more information.

4. From the Switcher drop-down list, select the required switcher. Specify the following details in the switcher settings.

Settings	Description
Primary Subrack ID	The ID that is associated while adding a switcher is displayed by default.
Input Number	Type the video input number on the subrack.

5. From the Digital Monitor -TV out, select the required monitor.
6. In the Connected To section, select the Recorder. See [Associating Recorder to a Video Input Device](#) for more information.

Note: Only Enterprise recorder can be associated.

7. Select Link if you want to broadcast the status changes and actions performed on the current video input device on the network.
8. Click Save.

Video Outputs

You can add various video output devices in MAXPRO VMS. You can add digital and analog monitors. The following types of video output devices are supported.

- Monitor – Analog and Digital.
- Standard Device – other devices, freeze frames and so on.
- Smart Device— devices such as multiplexers.
- Trunk - trunk video input (from a networked system).
- VCR – (video cassette recorder) - dedicated or Dub VCR.
- Standby VCR – Standby VCR as used in VCR Management.
- Digital Output Trunk – to view analog camera video.

Analog monitors are connected to the switchers and display video from analog cameras. The digital monitors are connected to the client workstations. Each client workstation can connect up to four digital monitors.

Video outputs and Partitions

A partition is a logical grouping of video devices. Partitions are associated to monitors. Monitors associated to a partition can be viewed or managed only by the users who are associated with it.

Video outputs and Event Groups

An event group is a set of events that occur on video devices. Event Groups are associated to monitors. An alarm is generated, When any event related to the monitor in the event group occurs.

Video outputs and Joystick Controller

Joystick controllers are associated to Monitors. Monitors associated to a joystick controller can be controlled by a user who is also associated with the joystick controller.

Adding Video Outputs

You can add digital and analog video outputs like monitors, smart devices, standard device, trunk, VCR, Standby VCR to display video. Video output devices like digital monitors are connected to the client workstations. The video output devices analog monitors are connected to the video matrix switchers.

Before you begin

- Add Site.
- Add Switcher (to associate the analog monitor).
- Add Workstation (to associate the digital monitor).
- Add Partition.
- Update Joystick Controller.

By default, a site and partition are available. You can associate the video outputs to them or create new.

To add a video output

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Outputs. The Video Output screen appears in the display area.

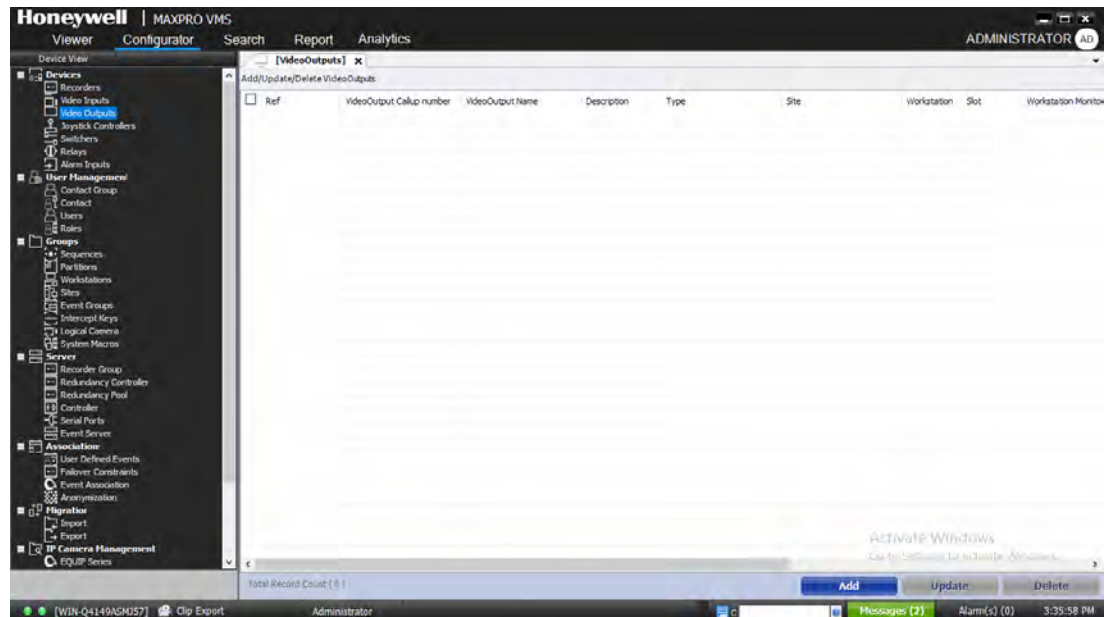


Figure 4-26 Video Outputs

3. Click Add. The Monitor screen appears by default.

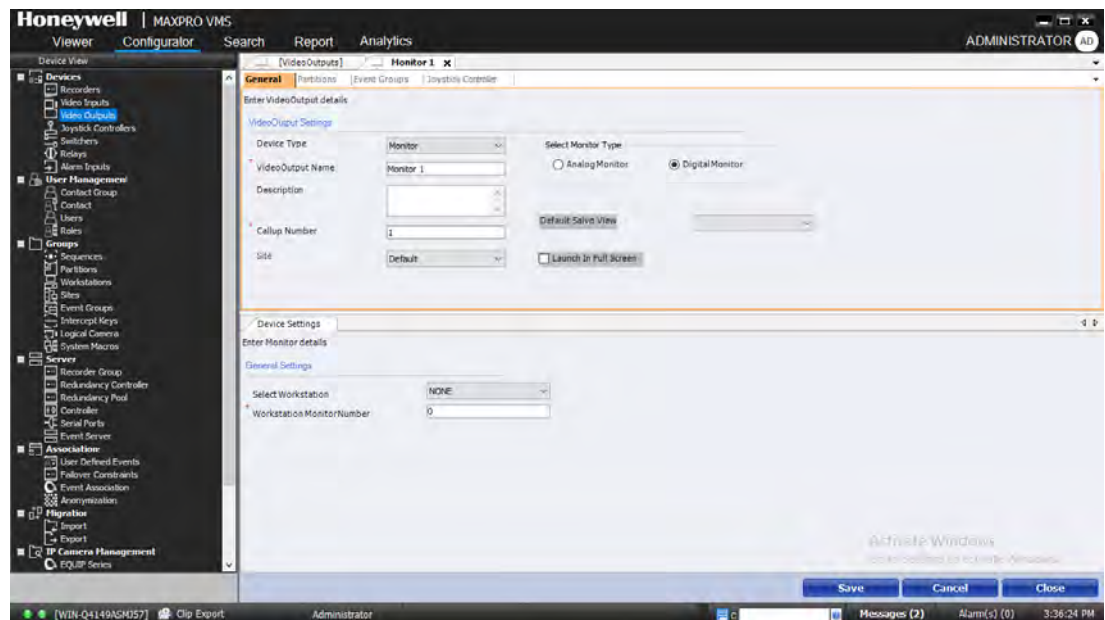


Figure 4-27 Monitors

4. From the Device Type drop-down list, select the required device type. The currently supported video output device types are listed in the following table. Click the corresponding links in the device column list to refer to the instructions while adding.
5. Associate Partition. See [Associating Partitions to Video Outputs](#) for more information.

Video Input Device	Description
Monitor	For details on configuring the monitor, see Adding Monitors .
Standard Device	For details on configuring the devices, see Adding a Video Output Device .
Smart Device	
VCR	
Standby VCR	
Trunk	For details on configuring the trunk, see Adding a Video Output Device (Trunk) .
Digital OutputTrunk	For details on configuring the digital output trunk, see Adding a Video Output Device (Digital Output Trunk) .

- Associate Joystick Controllers. See [Associating Video Outputs to Joystick Controllers](#).
- Associate Event Groups. See [Associating Video Outputs to Event Groups](#) for more information.
- Click Save.

Adding Monitors

Digital Monitor

To add a digital monitor

- Select the Digital Monitor under Select Monitor Type.
- In the VideoOutput Name box, type the name for the monitor.
- In the Description box, type a description for the monitor.
- In the Callup Number box, an automatic number is allocated by default. The operator uses this number to select a monitor from the keyboard.
- In the Site box, select the location in which the monitor is used.
- In the Default Salvo View drop-down list, select the default salvo view for the monitor.

Note: This feature helps in configuring the wall mounted digital monitors in a site to display live video from the selected salvo views.

- Select the Launch in Full Screen check box to launch the selected default salvo view in full screen mode, whenever the monitor is turned on.
- In the Select Workstation drop-down list in Device Settings area, select the workstation to which the monitor is connected.

9. In the Workstation Monitor Number box, type the number configured for the monitor during workstation setup.
10. Click Save.

Analog Monitor

To add a analog monitor

1. Select the Analog Monitor under Select Monitor Type.
2. In the VideoOutput Name box, type the name for the monitor.
3. In the Description box, type a description for the monitor.
4. In the Callup Number box, an automatic number is allocated by default. The operator uses this number to select a monitor from the keyboard.
5. In the Site box, select the location in which the monitor is used.
6. Select the Lock VideoOutput check box to lock monitor from displaying video.

Note: A monitor can be locked or unlocked by selecting or clearing the Lock VideoOutput check box. When a monitor is locked, no operations on the monitor are allowed including the multi monitor function.

7. In the Default Video Source box, type the camera callup number of the camera from which the live video is to be displayed.
8. In the Default Scan Sequence box, type the scan sequence number.
9. Select the Run Default Scan Sequence check box to automatically begin the default scan sequence.
10. In the Slot box, type the slot number to identify the slot location of the video output channel.
11. Click Switcher, if the monitor is connected to a switcher, and then select the required switcher in the Switcher drop-down list. Specify the following details.

Settings	Description
Text Inserter SubrackID	Address of the subrack that contains the text insertion card is displayed by default. The valid range of subrack addresses is 1 – 799; a value of 0 indicates the text is not used.
Text Inserter Slot	Type the slot number within the subrack where the text insertion card resides. The valid range of slot numbers is 1 – 32. HD Series hardware supports the MX208 8 channel video output/text insertion card, the text inserter slot entries correspond with the physical video output channel of the subrack. For VideoBloxsubrack, this number represents the physical input location of the video output channel. Valid range: 1 to 255 for VideoBlox.

12. Click the Net Device option, and then type the exact location and reference for the video

13. Select the LINK check box, if you want to broadcast the status changes and actions performed on the current video output device on the network.
14. In the Video Timeout box, type the display time-out period. The display time-out period can be set from 1-999 seconds. Enter a value zero if this function is not required.
15. In the Text Line Settings area, select the check boxes according to your requirement to select text line settings. The following table lists the options.

Option	Description
Message Line	Defines the line where the Message Line text (Example, Warning message) is displayed.
Mode Line	Defines the line where the Mode text (Example, Scan mode) is displayed.
Source Description	Defines the line the Video Input device description is displayed.
Channel Description	Defines the line where the description for the video device is displayed.
Real Time Clock	Defines the line the Real Time Clock is displayed.

Note: Selecting the Select All check box selects all the Text Line Settings.

16. In the Text Display Settings area, select the check boxes to select the text display settings. The following table lists the options.

Option	Description
Enhanced Card	To enhance the appearance of the text display.
Hidden Text	To hide the text display on the monitor.
Shadow	To apply shadow affect for the text display.
BackGround	To apply background affect for the text display.
Reverse Black/White	To reverse black/white affect for the text display.
Double Height	To increase the height of text display on monitor.
Flash	To display blinking text on the monitor.

Note: Selecting the Select All check box enables all the Text Display Settings.

17. In the X and Y boxes, type a location for the text to appear on the monitor. Valid positions are 1 –13. X and Y coordinates represent the horizontal and vertical position respectively.
18. In the Device Macro Flags section, select the required fields to set the macro flag to True. This field allows for definition of the default cold boot state of the

macro flags for the current video input device. Click Select All to set all the macro flags to True.

19. Click Save.

Adding a Video Output Device

To add the video output devices such as Standard Device/Smart Device/VCR/Standby VCR:

1. In the VideoOutput Name box, type the name for the monitor.
2. In the Description box, type a description for the monitor.
3. In the Callup Number box, an automatic number is allocated by default. The operator uses this number to select a monitor from the keyboard.
4. In the Site box, select the location in which the monitor is used.
5. Select the Lock VideoOutput check box to lock monitor from displaying video.
6. In the Switcher Settings, type the Slot number to identify the slot location of the video output channel
7. In the Text Inserter Subrack Settings area, click Switcher, if the monitor is connected to a switcher, and then select the required switcher in the Switcher drop-down list. Specify the following details.

Settings	Description
Text Inserter SubrackID	Address of the subrack that contains the text insertion card is displayed by default. The valid range of subrack addresses is 1 – 799; a value of 0 indicates the text is not used.
Text Inserter Slot box	Type the slot number within the subrack where the text insertion card resides. The valid range of slot numbers is 1 – 32. HD Series hardware supports the MX208 8 channel video output/text insertion card, the text inserter slot entries correspond with the physical video output channel of the subrack. For VideoBloxsubrack, this number represents the physical input location of the video output channel. Valid range: 1 to 255 for VideoBlox.

8. In the Network Settings area:
 - Select the Net Device option, and then type the exact location and reference for the video.
 - Select the LINK check box, if you want to broadcast the status changes and actions performed on the current video output device on the network.
9. In the Video Timeout box, type the display time-out period. The display time-out period can be set from 1-999 seconds. Enter a value zero if this function is not required.

10. In the Text Line Settings area, select the check boxes according to your requirement to select text line settings. The following table lists the options.

Option	Description
Message Line	Defines the line where the Message Line text (Example, Warning message) is displayed.
Mode Line	Defines the line where the Mode text (Example, Scan mode) is displayed.
Source Description	Defines the line the Video Input device description is displayed.
Channel Description	Defines the line where the description for the video device is displayed.
Real Time Clock	Defines the line the Real Time Clock is displayed.

Note: Selecting the Select All check box selects all the Text Line Settings.

11. In the Text Display Settings area, select the check boxes to select the text display settings. The following table lists the options.

Option	Description
Enhanced Card	To enhance the appearance of the text display.
Hidden Text	To hide the text display on the monitor.
Shadow	To apply shadow affect for the text display.
BackGround	To apply background affect for the text display.
Reverse Black/White	To reverse black/white affect for the text display.
Double Height	To increase the height of text display on monitor.
Flash	To display blinking text on the monitor.

Note: Selecting the Select All check box enables all the Text Display Settings.

12. In the X and Y boxes, type a location for the text to appear on the monitor. Valid positions are 1 –13. X and Y coordinates represent the horizontal and vertical position respectively.
13. In the Device Macro Flags area, select the required Flag check boxes to set the macro flag to True. This field allows for definition of the default cold boot state of the macro flags for the current video input device. Click Select All to set all the macro flags to True.
14. Click Save.

Adding a Video Output Device (Trunk)

1. In the VideoOutput Name box, type the name for the monitor.
2. In the Description box, type a description for the monitor.
3. In the Callup Number box, an automatic number is allocated by default. The operator uses this number to select a monitor from the keyboard.
4. In the Site box, select the location in which the monitor is used.
5. Select the Lock VideoOutput check box to lock monitor from displaying video.
6. In the Slot box, type the slot number to identify the slot location of the video output channel.
7. In the Video Timeout box, type the display time-out period. The display time-out period can be set from 1-999 seconds. Enter a value zero if this function is not required.
8. In the Text Line Settings area, select the check boxes according to your requirement to select text line settings. The following table lists the options.

Option	Description
Message Line	Defines the line where the Message Line text (Example, Warning message) is displayed.
Mode Line	Defines the line where the Mode text (Example, Scan mode) is displayed.
Source Description	Defines the line the Video Input device description is displayed.
Channel Description	Defines the line where the description for the video device is displayed.
Real Time Clock	Defines the line the Real Time Clock is displayed.

Note: Selecting the Select All check box selects all the Text Line Settings.

9. In the Text Display Settings area, select the check boxes to select the text display settings. The following table lists the options.

Option	Description
Enhanced Card	To enhance the appearance of the text display.
Hidden Text	To hide the text display on the monitor.
Shadow	To apply shadow affect for the text display.
BackGround	To apply background affect for the text display.
Reverse Black/White	To reverse black/white affect for the text display.
Double Height	To increase the height of text display on monitor.

Option	Description
Flash	To display blinking text on the monitor.

Note: Selecting the Select All check box enables all the Text Display Settings.

Adding a Video Output Device (Digital Output Trunk)

1. In the VideoOutput Name box, type the name for the monitor.
2. In the Description box, type a description for the monitor.
3. In the Callup Number box, an automatic number is allocated by default. The operator uses this number to select a monitor from the keyboard.
4. In the Site box, select the location in which the monitor is used.
5. Select the Lock VideoOutput check box to lock monitor from displaying video.
6. In the Slot box, type the slot number to identify the slot location of the video output channel.
7. In the Video Timeout box, type the display time-out period. The display time-out period can be set from 1-999 seconds. Enter a value zero if this function is not required.
8. In the Text Line Settings area, select the check boxes according to your requirement to select text line settings. The following table lists the options.

Option	Description
Message Line	Defines the line where the Message Line text (Example, Warning message) is displayed.
Mode Line	Defines the line where the Mode text (Example, Scan mode) is displayed.
Source Description	Defines the line the Video Input device description is displayed.
Channel Description	Defines the line where the description for the video device is displayed.
Real Time Clock	Defines the line the Real Time Clock is displayed.

Note: Selecting the Select All check box selects all the Text Line Settings.

9. In the Text Display Settings area, select the check boxes to select the text display settings. The following table lists the options.

Option	Description
Enhanced Card	To enhance the appearance of the text display.

Option	Description
Hidden Text	To hide the text display on the monitor.
Shadow	To apply shadow affect for the text display.
BackGround	To apply background affect for the text display.
Reverse Black/White	To reverse black/white affect for the text display.
Double Height	To increase the height of text display on monitor.
Flash	To display blinking text on the monitor.

Note: Selecting the Select All check box enables all the Text Display Settings.

10. In the X and Y boxes, type a location for the text to appear on the monitor. Valid positions are 1 –13. X and Y coordinates represent the horizontal and vertical position respectively.
11. In the Device Macro Flags section, select the required fields to set the macro flag to True. This field allows for definition of the default cold boot state of the macro flags for the current video input device. Click Select All to set all the macro flags to True.
12. Specify the Video Source in the Digital Settings tab.

Option	Description
Video Source	From the drop-down list, select the required video input device to display video.

Deleting a Video Output Device

To delete a video output device

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Outputs. The Video Outputs screen appears in the display area.
3. Select the check box corresponding to the video output device that you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Updating a Video Output Device

You can update a video output device to change its association with a partition, joy-stick controller, and also to modify its settings.

To update a video output

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Outputs. The Video Outputs screen appears in the display area.
3. Select the check box corresponding to the video output you want to update.
4. Click Update. The settings for the video output appear. You can modify the settings.
5. Click Save.

Locking the Display on the Monitor

The analog monitor can be locked to display the video only from a particular camera and field of view. The operator cannot perform pan, tilt, or zoom using a monitor with locked display.

To lock the display on a monitor

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Outputs. The Video Outputs screen appears in the display area.
3. Select the check box corresponding to the monitor you want to lock.
4. Double-click or click Update. The General Settings for the monitor appears.
5. Select the Lock VideoOutput check box.
6. Click Save.

Associating Partitions to Video Outputs

You can add partitions to video outputs. A video output associated with a partition can be viewed and managed by a user who is in turn associated with the partition.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partitions to video outputs

1. Click the Partitions tab. The screen displays the associated partitions, if any.
2. Click Associate. The Select Partitions page appears.
3. Select the check box corresponding to the partition name you want to associate.
4. Click OK. The selected partition is displayed in the list of associated partitions.

To disassociate partition from the video outputs

- Select the check box corresponding to the partition name, and then click Remove.

Associating Video Outputs to Event Groups

You can associate event groups to video outputs. Associating video outputs to event groups allows display of alarms that are associated with the event group.

Before you begin

- Add Event Group.

To associate event groups to video outputs

1. Click the Event Groups tab. The screen displays the associated event groups, if any.
2. Click Associate. The Select Event Groups page appears.
3. Select the check box corresponding to the Event Group name you want to associate.
4. Click OK.

To disassociate event groups from video outputs

- Select the check box corresponding to the Event Group name, and then click Remove.

Associating Video Outputs to Joystick Controllers

You can associate Joystick Controllers to monitors. Monitors associated to a joystick controller can be controlled by a user who is also associated with the joystick controller.

Before you begin

- Update Joystick Controller.

To associate joystick controllers to video output

1. Click the Joystick Controller tab. The screen displays the associated joysticks if any.
2. Click Associate. The Select Joystick Controller page appears.
3. Select the check box corresponding to the joystick name you want to associate.
4. Click OK.

Note: *By default, all the joystick controllers are associated when a user is added. You can remove the joystick that you do not require.*

To disassociate Joystick Controller from a video output

- Select the check box corresponding to the joystick name, and then click Remove.

Joystick Controllers

An Ultrakey keyboard is referred to as the joystick controller. Using the Ultra key 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. You can program the keys in the Ultrakey keyboard to perform a particular action by associating intercept commands to them. For example, a key can be programmed to select a panel in the salvo layout.

By default, 99 keyboards and a server keyboard is added. Only joystick controller 1 is enabled by default. The server keyboard cannot be deleted.

Joystick Controllers and Users

Users are responsible for carrying out video surveillance operations in MAXPRO VMS. Joystick controllers are associated to users. Users associated to joystick controllers can carry out video surveillance tasks in the client workstations.

Joystick Controllers and Intercept Keys

Joystick controllers (Ultrakey keyboards) are associated to intercept keys. You can program the keys in the Ultrakey keyboard to perform an action by associating intercept keys to them. For example, a key can be programmed to select a panel in the salvo layout.

Joystick Controllers and Video Outputs

Joystick controllers are associated to video outputs in MAXPRO VMS

Configuring joystick controller

To enable the joystick controller on the MAXPRO VMS, you need to configure the joystick controller.

To configure the joystick controller

1. Press ALT + Home in Joystick Controller. The STARTUP Menu of the configuration page appears.
2. On the STARTUP MENU screen, press Configure. The Numeric Entry screen appears.
3. In the Enter Your Password box, type the password, and then press Enter. The Configuration screen appears.
4. Press HardwareConfig. The HARDWARE CONFIG screen appears.
5. Press Port Settings. The PORT SETUP screen appears.
6. Press Ethernet. The ETHERNET SETUP screen appears.
7. Press IP Address, and then type the IP Address of the Joystick Controller.
8. Press Subnet Mask, and then type the Subnet Mask of the network.

9. Press Default Gateway, select the required Gateway.
10. Press Sys.Cntl. IP Address, and then type the IP address of the MAXPRO™ VMS Server.
11. Press Save.
12. Press Quit to return to the STARTUP Menu screen.
13. In the STARTUP Menu, press Run.

Connecting the Keyboard to MAXPRO VMS

To connect a keyboard to MAXPRO VMS

1. Go to C:\Program Files\Honeywell\TrinityFramework\bin, the default path where MAXPRO VMS is installed.
2. Double-click MAXPRO_Keyboard_Prototype.exe. The Simulator page appears.
3. In the Keyboard Number box, type the input number for the keyboard.
4. In the IP Address box, type the IP address of the MAXPRO™ VMS Server.
5. Click Power-On.

Sign On and Sign Off

Before you sign on and sign off from a joystick controller, you must configure the features.

Configuring the Sign On and Off feature

To configure the sign on and off feature

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Joystick Controllers. The Joystick Controllers screen appears in the display area.

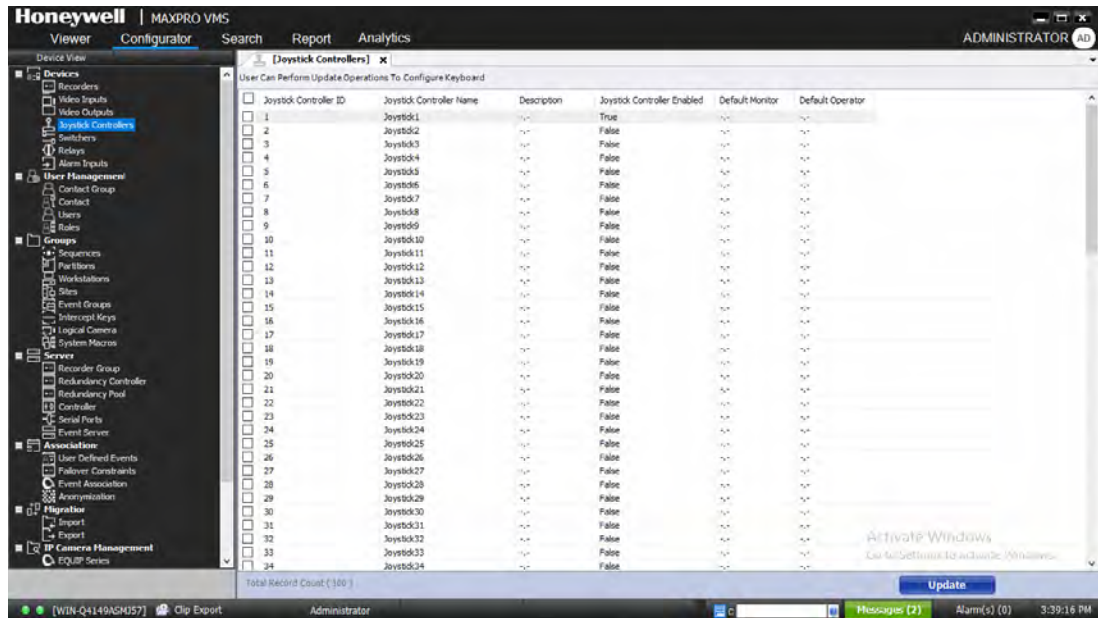


Figure 4-28 Joystick Controller

3. Double-click the joystick controller for which you want to use the sign on and sign off feature. The joystick screen appears.
4. In the Default Operator drop-down list, select None.
5. Click Save.
6. Restart the trinity services.
7. Create an ultrakey button for menu whose intercept key value is 41. For more information on creating a ultrakey button, refer to the ultrakey user manual.

Note: By default, the intercept key 41 is defined in MAXPRO VMS and the replacement macro is “?”.

To sign on to the joystick controller

1. Press the Menu button on the joystick controller.
2. Select the operator number, and then press Enter. You are prompted to enter the four digit pin.
3. Type the four digit pin, and then press Enter.

Note: You can see the names directly on the display.

To sign off from the joystick controller

1. Press the Menu button on the joystick controller.
2. Press the PTZ tilt down button, and then press Enter. A message asking for confirmation appears.
3. Press Enter.

Updating a Joystick Controller

You can update a joystick controller to modify the keyboard settings.

To update a joystick controller

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Joystick Controllers. The Joystick Controllers screen appears in the display area.
3. Select the check box corresponding to the joystick controller you want to update, and then click Update. The Enter Keyboard details screen appears.

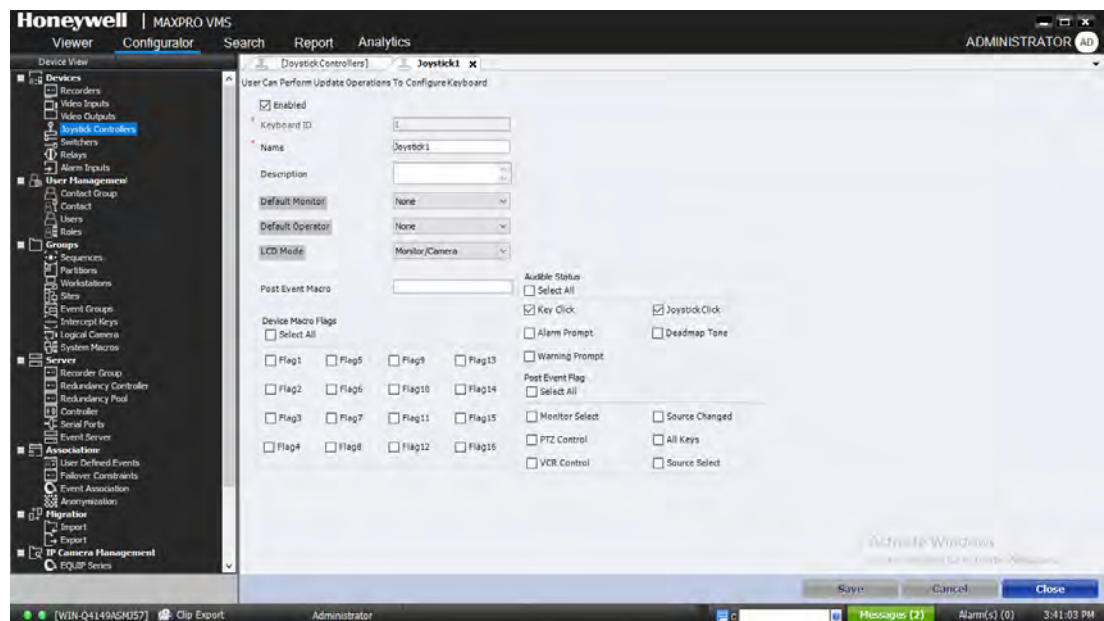


Figure 4-29 Updating a Joystick Controller

4. In the Enter Keyboard Details area, select the Enabled check box. The Keyboard ID is displayed automatically.
5. In the Name box, type the name for the keyboard.
6. In the Default Monitor drop-down list, select the default monitor to be associated with the joystick controller.
7. In the Default Operator drop-down list, select the default user to be associated with the joystick controller.
8. In the LCD Mode drop-down list, select the LCD display mode.

9. In the Audible Status area, select the check boxes to configure audible keyboard prompts. The following table lists the audible status options.

Option	Description
Key Click	The keyboard beeps in response to every key press.
Joystick Click	The keyboard beeps in response to any joystick movement.
Warning Prompt	The keyboard buzzes in response to warning messages.
Alarm Prompt	The keyboard beeps continuously in response to an alarm message, until the alarm is cleared.
Deadmap Tone	The keyboard beeps if it is not used for specific amount of time, as defined by keyboard operator section.

Note: Selecting the Select All check box enables all the options.

10. In the Post Event Macro box, type the Macro number to be executed after an event.
11. In the Post Event Flag area, select the check boxes to select the type of events that triggers the post event macro. The following table lists the post event flag options.

Option	Description
Monitor Select	The post event macro is executed every time a monitor is selected.
Source Select	The post event macro is executed every time a video input device is selected.
Source Changed	The post event macro is executed every time a different video input device is selected on the keyboard's current monitor.
PTZ Control	The post event macro is executed every time the keyboard is used for control of a PAN/TILT/ZOOM camera.
VCR Control	The post event macro is executed every time the keyboard is used for control of a VCR.
All Keys	The post event macro is executed for every key press on the keyboard.

Note: Selecting the Select All check box enables all the options.

12. In the Device Macro Flags area, select the check boxes to set and test from within the macro environment.
13. Click Save.

Switchers

Switcher routes multiple analog camera inputs to multiple analog monitor outputs.

Switchers and Partitions

A partition is a logical grouping of video devices. Partitions are associated to switchers. You can restrict a non-associated user of the partition from viewing or changing the settings of the switcher.

Switchers and Events

Events are predefined actions. Switchers have predefined events by default. An alarm is triggered whenever an event is generated. For example, when a switcher is disconnected, an event 'Connection lost' is generated.

Adding a Switcher

You can add a switcher to route video input (analog camera) to a video output (analog monitor).

Before you begin

- Add Site. See [Adding a Site](#) for more information.
- Add Partition. See [Adding a Partition](#) for more information.
- Add Event Groups. See [Adding an Event Group](#) for more information.
- Add Serial Ports. See [Adding a Serial Port](#) for more information.

By default, a site, partition and event groups are available. You can associate the switcher to them or create new.

To add a switcher

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Switchers. The Switchers screen appears in the display area.

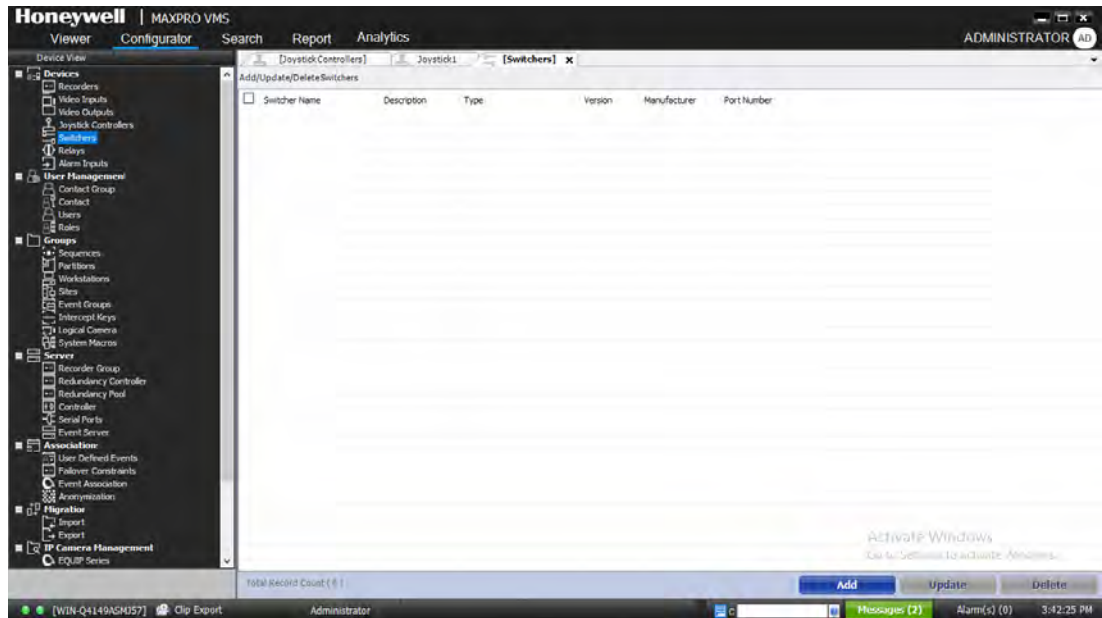


Figure 4-30 Switchers

3. Click Add. The General Settings appear.

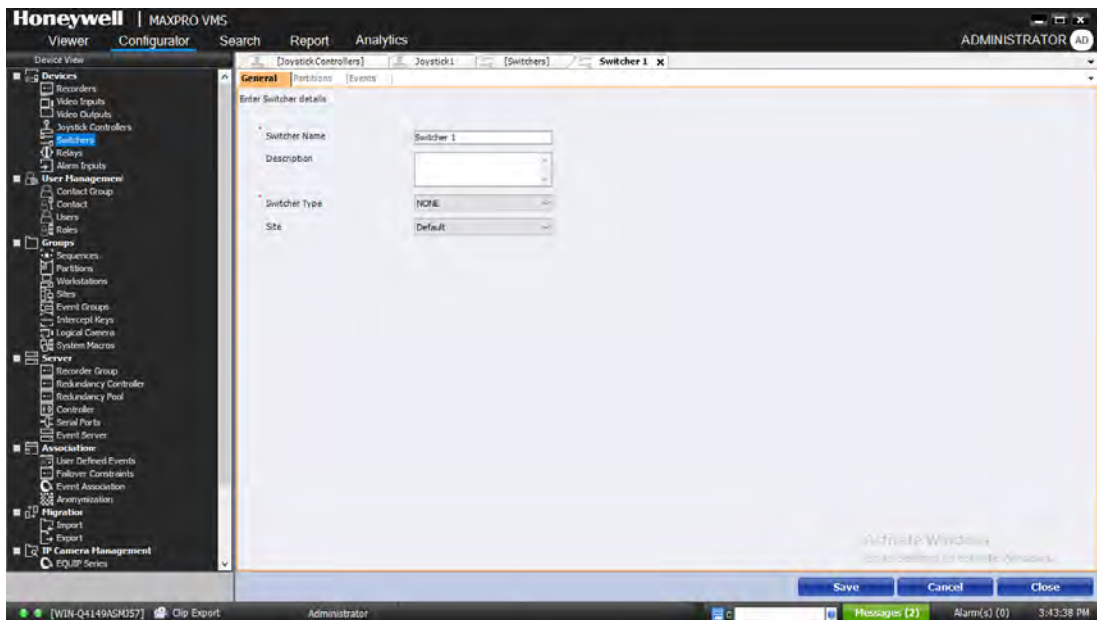


Figure 4-31 Switcher General Settings

4. In the Switcher Name box, type the name of the switcher.
5. In the Description box, type a description for the switcher.
6. In the Switcher Type drop-down list, select the type of switcher. The following are the available type of switchers.

- Vicon
- Burle
- AmericanDynamics
- PelcoSwitcher
- VideoBlox
- MaxPro

Note: Selecting “MaxPro” enables the Primary Subrack ID box.

7. In the Primary Subrack ID box, type the address of the subrack.

Note: Valid primary subrack addresses range from 1 – 99. A value of '0' indicates that no video switching occurs when the device is selected. For VideoBlox subrack, this ID represents the 'V'+communication port number to which the VideoBlox analog video input cards are connected. The valid primary subrack address is 'V'+maximum communication ports. Suffix 'A' with primary subrack ID (for example, V1A) indicates that the audio is enabled for that particular video input.

8. From the Site drop-down list, select the location to which you want to connect the switcher.
9. From the Choose the COM Port drop-down list, select the required port. See also, Configuring Switchers. See [Configuring Switchers](#) for more information.
10. Associate Partition. See [Associating Partitions to Switcher](#) for more information.
11. Associate Events. See [Associating Events to Switcher](#) for more information.
12. Click Save.

Configuring Switchers

This section details the sequential procedure to configure the switchers that are supported by MAXPRO VMS.

Before you begin

- Add a Serial Port.
- Configuring the Switcher

1. Click the Configurator tab.
2. Expand Server in the navigation area, and then click Serial Ports. The Serial Ports screen appears in the display area.
3. Click Add. A Joystick screen appears. Refer to the instructions in the table to configure the port for various switchers.
4. Click Save.

Note: For more information on adding serial ports, see [Adding a Serial Port](#) section.

Switchers	Instructions
Vicon	<ul style="list-style-type: none"> • In the COM Port Number, type the reference number of the serial port. • In the Port Name type a name for the port. • In the Port Type drop-down list, select the port type as NONE. • In the Baud Rate drop-down list, select 9600. • In the Data Bit drop-down list, select EIGHT. • In the Stop Bit drop-down list, select ONE. • In the Parity drop-down list, select NONE.
Burle	<ul style="list-style-type: none"> • In the COM Port Number, type the reference number of the serial port. • In the Port Name type a name for the port. • In the Port Type drop-down list, select the port type as NONE. • In the Baud Rate drop-down list, select 9600. • In the Data Bit drop-down list, select EIGHT. • In the Stop Bit drop-down list, select ONE. • In the Parity drop-down list, select NONE.
Pelco	<ul style="list-style-type: none"> • In the COM Port Number, type the reference number of the serial port. • In the Port Name type a name for the port. • In the Port Type drop-down list, select the port type as NONE. • In the Baud Rate drop-down list, select 9600. • In the Data Bit drop-down list, select EIGHT. • In the Stop Bit drop-down list, select ONE. • In the Parity drop-down list, select an odd parity
MaxPro	<ul style="list-style-type: none"> • In the COM Port Number, type the reference number of the serial port. • In the Port Name type a name for the port. • In the Port Type drop-down list, select the port type as NONE. • In the Baud Rate drop-down list, select 19200. • In the Data Bit drop-down list, select SEVEN. • In the Stop Bit drop-down list, select ONE. • In the Parity drop-down list, select an even parity

Switchers	Instructions
American Dynamics	<ul style="list-style-type: none"> • In the COM Port Number, type the reference number of the serial port. • In the Port Name type a name for the port. • In the Port Type drop-down list, select the port type as NONE. • In the Baud Rate drop-down list, select 19200. • In the Data Bit drop-down list, select SEVEN. • In the Stop Bit drop-down list, select ONE. • In the Parity drop-down list, select an even parity
VideoBlox	<ul style="list-style-type: none"> • In the COM Port Number, type the reference number of the serial port. • In the Port Name type a name for the port. • In the Port Type drop-down list, select the port type as NONE. • In the Baud Rate drop-down list, select 19200. • In the Data Bit drop-down list, select EIGHT. • In the Stop Bit drop-down list, select ONE. • In the Parity drop-down list, select NONE.

Adding a Switcher

To add a switcher

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Switchers. The Switchers screen appears in the display area.
3. Click Add. A Switcher screen appears.
4. In the Switcher Type drop-down list, select the required switcher.

Note: For more details on adding a switcher, see [Adding a Switcher](#) section.

Adding a Camera and Associating a Switcher

To add a camera and associate a switcher

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Cameras. The Cameras screen appears in the display area.
3. Click Save.
4. Click Add. A Camera screen appears.
5. In the Connected to area, click Switcher. The Switcher drop-down list is enabled and displays the configured switcher.
6. Select the required switcher. The Device Settings for the switcher appear.

7. For detailed procedures about associating the switcher to the camera, see [Associating a Switcher to a Video Input](#).

Note: You should have a camera physically connected to the input channel in the Vicon Switcher. In this case the camera must be physically connected to the channel 1.

Adding a Analog Monitor

To add an analog monitor

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Monitors. The Monitors screen appears in the display area.
3. Click Add. A Monitor screen appears.
4. In the Select Monitor Type, select Analog Monitor.
5. In the Monitor Name box, type a name for the monitor.

Note: The camera number and the monitor number must be same. For example if you want the video output of camera number 1, then the monitor number must be 1.

6. Under the Device Settings, in the Select Switcher drop-down list, select the required switcher.
7. For detailed procedures about associating the switcher to the camera, see [Adding Monitors](#).
8. Click Save.

Associating a Joystick Controller

To associate a joystick controller

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Joystick Controllers. The Joystick Controllers screen appears in the display area.
3. Select the check box corresponding to the Joystick Controller, and then click Update. A Joystick Controller screen appears.
4. In the Default Monitor drop-down list, select the default monitor to be associated with the joystick controller. For example, if the monitor number is one to which you have associated the required switcher, then select Monitor 1 as the default monitor.
5. In the Default Operator drop-down list, select the default user to be associated with the joystick controller.

Note: An operator must be added before you add a joystick controller.

6. Click Save.

After these settings are made in MAXPRO VMS, restart the Trinity Services.

Note: Check whether you are able to drag and drop configured cameras on to the monitor.

Updating a switcher

You can update a switcher to change or edit the settings like the recorder name, site and COM port.

To update a switcher

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Switchers. The Switchers screen appears in the display area.
3. Select the check box corresponding to the switcher you want to update.
4. Click Update. The general settings for the switcher appears. You can modify the settings according to your needs.

Deleting a switcher

To delete a switcher

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Switchers. The Switchers screen appears in the display area.
3. Select the check box corresponding to the switcher you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Associating Partitions to Switcher

You can associate partitions to switcher. Associating a partition to a switcher restricts a non- associated user of the partition from viewing the switcher or changing the settings of the switcher.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partitions to a switcher

1. Click the Partitions tab. The screen displays the associated partitions, if any.

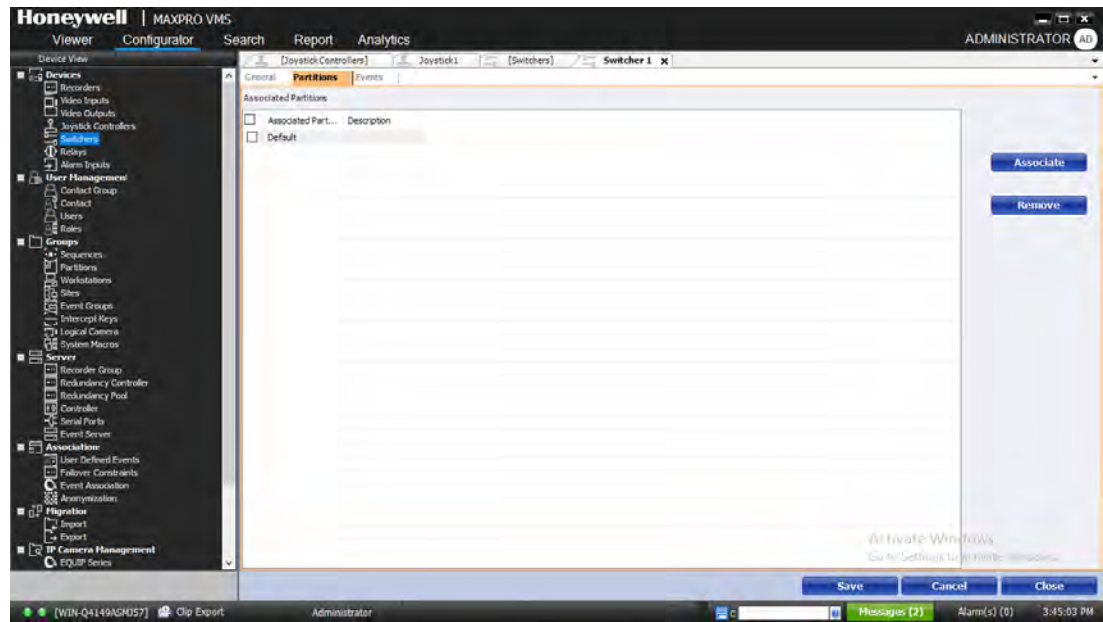


Figure 4-32 Switcher Partitions

2. Click Associate. The Select Partitions page appears.
3. Select the check box corresponding to the partition name you want to associate.
4. Click OK.

To disassociate partitions from switcher

- Select the check box corresponding to the partition name, and then click Remove.

Associating Events to Switcher

You can associate events to switcher. An alarm is triggered whenever an event occurs.

To associate events to a switcher

1. Click the Events tab. The screen displays the associated events, if any.

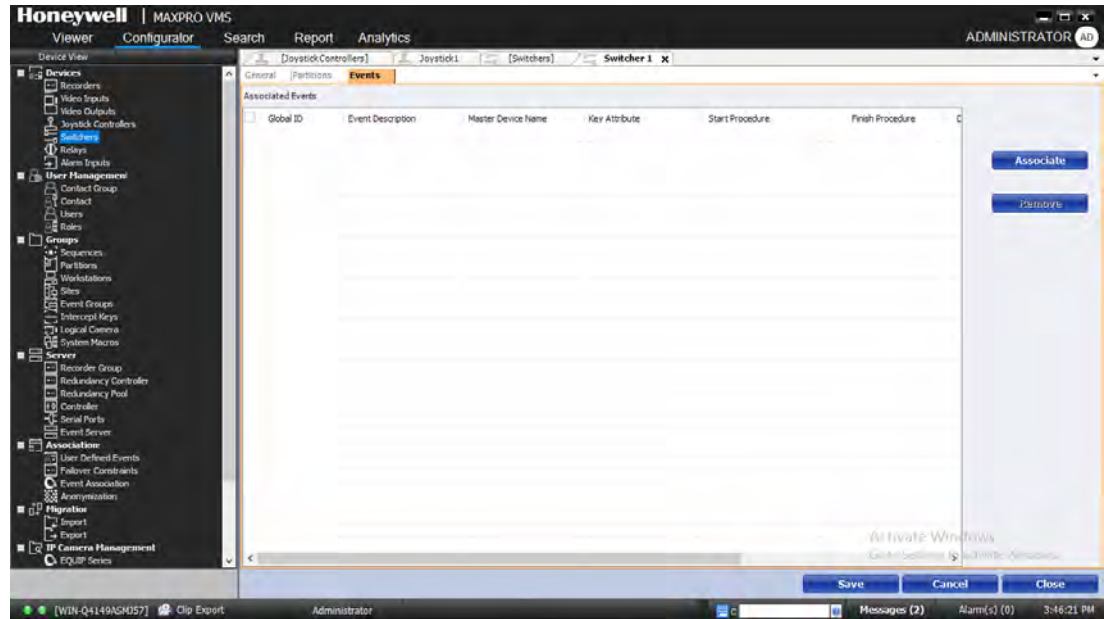


Figure 4-33 Switcher Events

2. Click Associate. The Select Available Events page appears.
3. Select the check box corresponding to the event you want to associate.
4. Click OK.

To disassociate events from a switcher

- Select the check box corresponding to the event, and then click Remove.

To add event groups to events

1. Select the check box corresponding to the event you want to add the Event Group.
2. Double-click on the Event Group box. Select Event Groups page appears.
3. Click the check box corresponding to the Event Group you want to add.
4. Click OK.

Note: You need to add an event group before you associates it to an event. See [Adding an Event Group](#) for more information.

To disable an event

1. Select the check box corresponding to the event you want to disable.
2. Click the cell under the Disabled column. A drop-down list is enabled.
3. Select True to disable the event.

To assign severity level

1. Select the check box corresponding to the event you want to assign the severity level.
2. Click the cell under the Severity Level column and edit the severity level.

Note: *Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.*

To enter remarks

1. Select the check box corresponding to the event you want to enter remarks.
2. Click the cell under the Remarks column and type the remarks.
3. Type the remarks you want to enter.

To assign macros

1. Select the check box corresponding to the event you want to assign macros.
2. Click the cell under the Start Procedure column, and then type the required macro.
3. Click the cell under the End Procedure column, and then type the required macro.

Relays

Relay is an output contact that can be triggered from MAXPRO VMS. Relays can be connected to devices like switcher, recorder, cameras, keyboard, and high level device. Relays send signals that perform various actions. For example, you can set a relay to open the door automatically when a motion is detected in a particular region.

Adding the relay

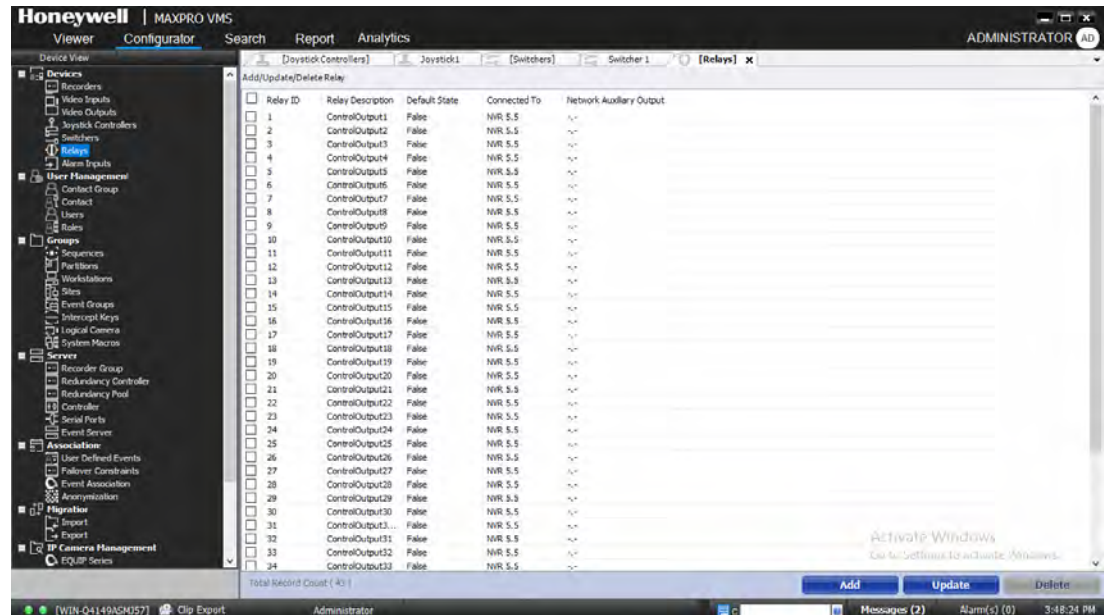
Before you begin

- Add Site. See [Adding a Site](#) for more information.
- Add Switcher. See [Adding a Switcher](#) for more information.
- Add Recorder. [Adding a Recorder](#) for more information.
- Add Partition. See [Adding a Partition](#) for more information.
- Update Joystick Controller. See [Updating a Joystick Controller](#) for more information.

By default, a site and a partition are available. You can associate the relay to them or create new.

To add a relay

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Relays. The Relays screen appears in the display area.



3. Click Add. The Relay screen appears.

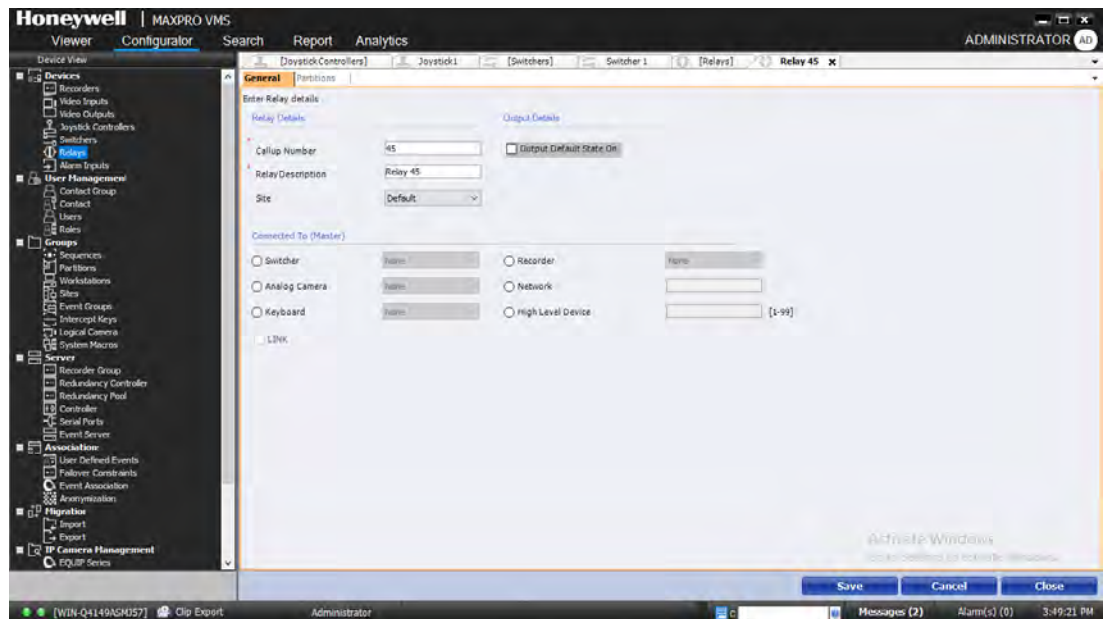


Figure 4-34 Relays General

4. In the Callup Number box, type the unique ID to identify the relay. By default MAXPRO VMS assigns the next available ID.
5. In the Relay Description box, type a description for the relay.
6. In the Site drop-down list, select the site.

7. In the Connected To section, click one of the devices from which you want to add a relay. The following table lists the available devices to which a relay can be connected.

Device	Description
Switcher	For details on connecting to a switcher, see Connecting Relay to the Switcher .
Analog Camera	For details on connecting to an analog camera, see Connecting Relay to the Analog Camera .
Keyboard	For details on connecting to a keyboard, see Connecting the relay to Keyboard .
Recorder	For details on connecting to a recorder, see Connecting the relay to the Recorder .
Network	For details on connecting to a network, see Connecting Relay to the Network .
High Level Device	For details on connecting to a high level device, see Connecting Relay to the High Level Device .

8. Select the LINK check box if you want to broadcast the status changes and actions performed on the current relay on the network.
9. Select the Output Default State On check box if you want the relay to be set to On, when the MAXPRO VMS is started.
10. Associate Partitions.
11. Click Save. The Trigger Relay options appear.
12. Click On to trigger relay.
13. Click Off to stop relay.

Connecting Relay to the Switcher

Before you begin

- Add Switchers. See [Adding a Switcher](#) for more information.

To connect relay to a switcher

1. From the Switcher drop-down list, select the required switcher. The Switcher Settings appear.

Note: In the SubrackID box, the Subrack ID number where the relay module resides is displayed automatically. The valid range is 1 – 99. If a high level or mimic panel output is used, the number is prefixed with an “H”. If a keyboard output is used, the number is prefixed with a “K”. For VideoBlox subrack, this represents the ‘V’+communication port number to which the VideoBlox alarm concentrator AVBPIT is connected. Valid range: ‘V’+maximum communication ports.

2. In the Subrack Slot, type a slot number within the control subrack where the control output module resides.

Note: The valid slot numbers are 1 – 32 for I/O and combination video/I/O subracks, and 1 for HD Series subracks. For VideoBlox subrack, this represents the physical control input slot number from AVBPIT alarm concentrator. Valid range is 1 to 255.

3. In the Output Bit section, select the required output that needs to be controlled by the relay. Each relay can control one or more output bits. Click Select All if you want all the output bits to be controlled by a single relay.
4. Click Save.

Connecting Relay to the Analog Camera

Before you begin

- Add Cameras. See [Adding a Camera](#) for more information.

To connect relay to an analog camera

1. From the Analog Camera drop-down list, select the required camera. The Device Settings appears.

Note: In the SubrackID box, the Subrack ID number where the relay module resides is displayed automatically. The valid range is 1 – 99. If a high level or mimic panel output is used, the number is prefixed with an “H”. If a keyboard output is used, the number is prefixed with a “K”. For VideoBlox subrack, this represents the ‘V’+communication port number to which the VideoBlox alarm concentrator AVBPIT is connected. Valid range: ‘V’+maximum communication ports.

2. In the Output Bit section, select the required output that needs to be controlled by the relay. Each relay can control one or more output bits. Click Select All if you want all the output bits to be controlled by a single relay.

Note: In the Subrack Slot, the slot number within the control subrack where the control output module resides is displayed automatically. The valid slot numbers are 1 – 32 for I/O and combination video/I/O subracks, and 1 for HD Series subracks. For VideoBlox subrack, this represents the physical control input slot number from AVBPIT alarm concentrator. Valid range is 1 to 255.

3. Click Save.

Connecting Relay to the High Level Device

To connect relay to a high level device

1. In the High Level Device box, type the device number. The Device Settings appear.
2. In the SubrackID box, type the Subrack ID number where the relay module resides.

Note: The valid range is 1 – 99. If a high level or mimic panel output is used, the number is prefixed with an “H”. If a keyboard output is used, the number is prefixed with a “K”. For VideoBlox subrack, this represents the ‘V’+communication port number to which the VideoBlox alarm concentrator AVBPIT is connected. Valid range is ‘V’+maximum communication ports.

3. In the Subrack Slot, the slot number within the control subrack where the control output module resides is displayed automatically.

Note: The valid slot numbers are 1 – 32 for I/O and combination video/I/O subracks, and 1 for HD Series subracks. For VideoBlox subrack, this represents the physical control input slot number from AVBPIT alarm concentrator. Valid range is 1 to 255.

4. In the Output Bit section, select the required output that needs to be controlled by the relay. Each relay can control one or more output bits. Click Select All if you want all the output bits to be controlled by a single relay.
5. Click Save.

Connecting Relay to the Network

To connect relay to a network

1. In the Network box, type the network node and the video input device number from which you want the video input.
2. Click Save.

Connecting the relay to the Recorder

Before you begin

- Add Recorders. See [Adding a Recorder](#) for more information.

To connect relay to a analog camera

1. From the Recorder drop-down list, select the required recorder. The Output Settings appear.
2. In the Relay ID box, type the relay ID number for the recorder.
3. In the Site ID box, type the site ID of the recorder.
4. In the Station ID box, type the station ID of the recorder.
5. In the Digital IO Type, type the digital IO type of the recorder.
6. In the Output Bit section, select the required output that needs to be controlled by the relay. Each relay can control one or more output bits. Click Select All if you want all the output bits to be controlled by a single relay.

7. Click Save.

Note: Steps 3 through 9 are required only when you are connecting to Enterprise recorder.

Connecting the relay to Keyboard

To connect relay to a keyboard

1. From the Keyboard drop-down list, select the required joystick controller. The Device Settings appear.

Note: In the SubrackID box, the Subrack ID number where the relay module resides is displayed automatically. The valid range is 1 – 99. If a high level or mimic panel output is used, the number is prefixed with an “H”. If a keyboard output is used, the number is prefixed with a “K”. For VideoBlox subrack, this represents the ‘V’+communication port number to which the VideoBlox alarm concentrator AVBPIT is connected. Valid range is ‘V’+maximum communication ports.

2. In the Output Bit section, select the required output that needs to be controlled by the relay. Each relay can control one or more output bits. Click Select All if you want all the output bits to be controlled by a single relay.

Note: In the Subrack Slot, the slot number within the control subrack where the control output module resides is displayed automatically. The valid slot numbers are 1 – 32 for I/O and combination video/I/O subracks, and 1 for HD Series subracks. For VideoBlox subrack, this represents the physical control input slot number from AVBPIT alarm concentrator. Valid range is 1 to 255.

3. Click Save.

Associating Partitions to the Relay

You can associate partition to relay. Associating a partition to a relay restricts a non-associated user of the relay from changing the settings of the relay.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partitions to relay

1. Click the Partitions tab. The screen displays the associated partitions, if any.

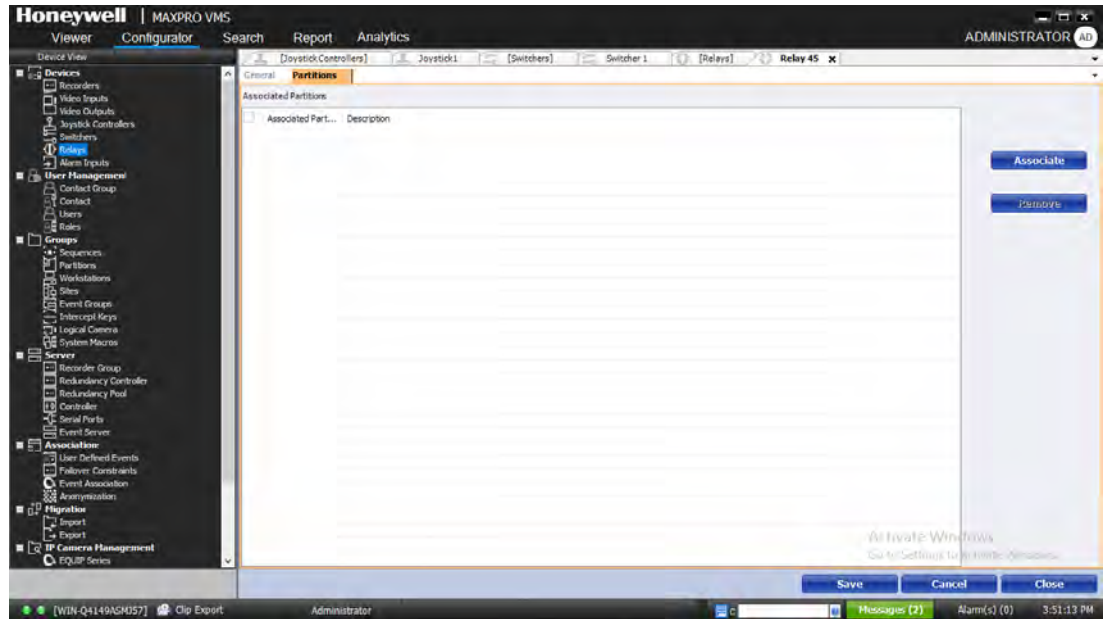


Figure 4-35 Relays Partitions

2. Click Associate. The Select Partitions page appears.
3. Select the check box corresponding to the partition name you want to associate.
4. Click OK. The selected partition is displayed in the list of associated partitions.

To disassociate partitions to relay

- Select the check box corresponding to the partition name, and then click Remove.

Deleting the Relay

You can delete a relay when you no longer want to trigger a task that is based on a relay.

Before you begin

- Disassociate Partitions. [Associating Partitions to the Relay](#) for more information.

To delete a relay

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click relays. The Relays screen appears in the display area.
3. Select the check box corresponding to the relay that you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Updating the Relay

You can update a relay device to change its association with a partition and also to modify its settings.

To update a relay

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click relays. The Relays screen appears in the display area.
3. Select the check box corresponding to the relay you want to update.
4. Click Update. The settings for the relay appear. You can modify the settings.

Alarm Inputs

Alarm inputs are used to raise alarms through an external device in MAXPRO VMS. These alarm inputs can be associated to devices like switcher, recorder, camera, keyboard, network and high level device.

Adding an Alarm Input

You can add an alarm input and associate it to the devices. These alarm inputs trigger alarm whenever an event occurs.

Before you begin

- Add Site. See [Adding a Site](#) for more information.
- Add Switcher. See [Adding a Switcher](#) for more information.
- Add Recorder. [Adding a Recorder](#) for more information.
- Add Partition. See [Adding a Partition](#) for more information.
- Update Joystick Controller. See [Updating a Joystick Controller](#) for more information.

By default, a site and a partition are available. You can associate the alarm input to them or create new.

To add an alarm input

1. Click the Configurator tab.
2. Expand the Devices branch in the navigation area, and then click Alarm Inputs. The Alarm Input screen appears in the display area.

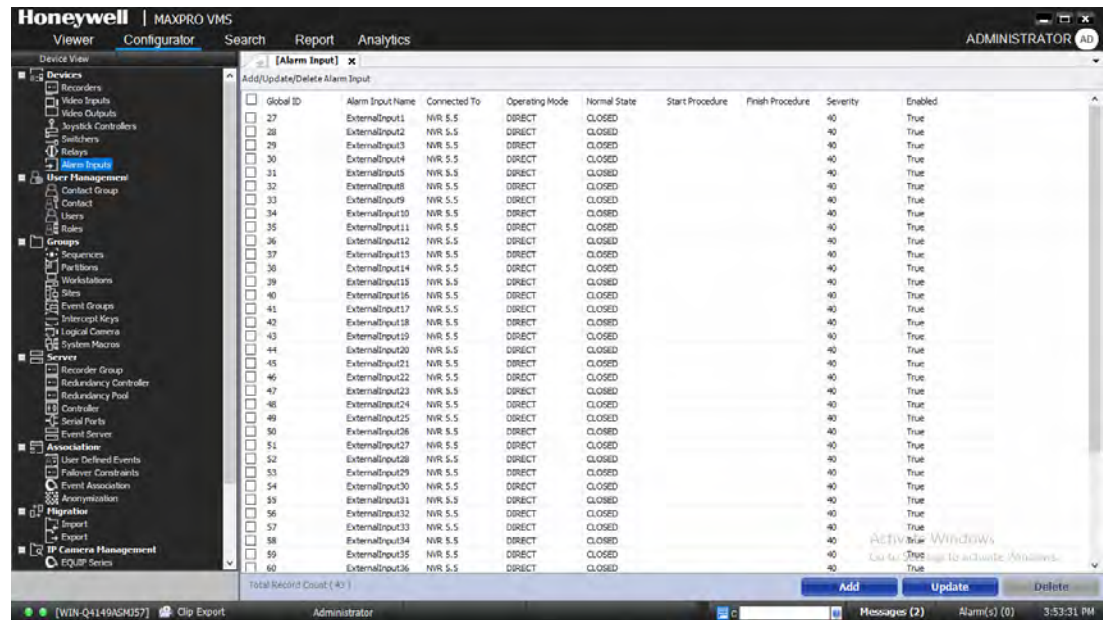


Figure 4-36 Alarm Input

3. Click Add. The Alarm Input screen appears.

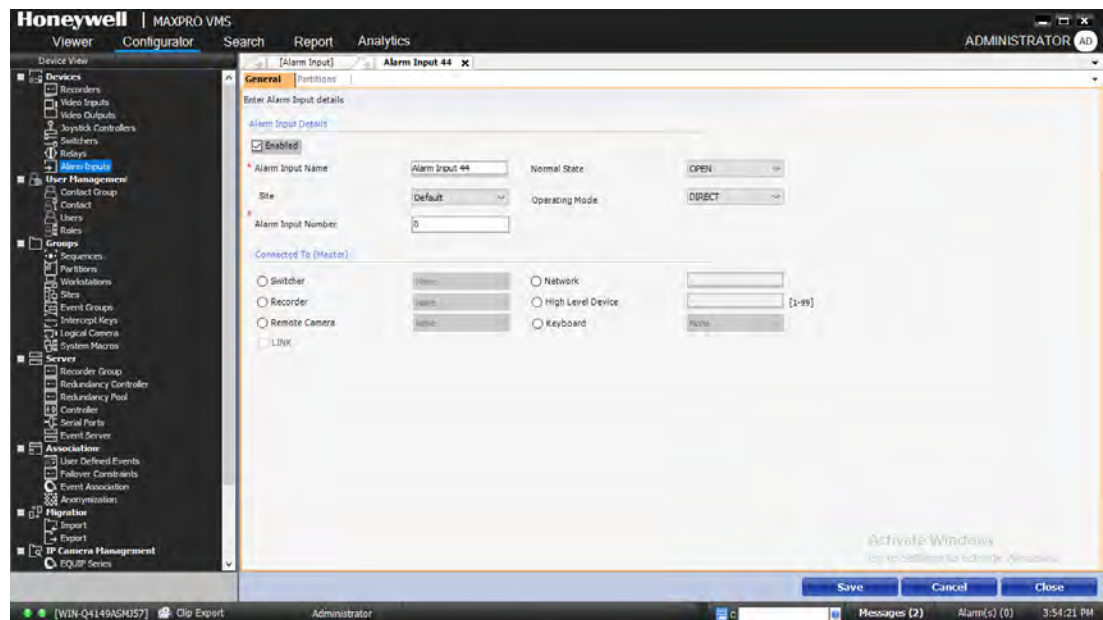


Figure 4-37 Adding an Alarm Input

4. The Enabled check box is selected by default. Clear this check box to disable the alarm input.
5. In the Alarm Input Name box, type the alarm input name.

6. From the Site drop-down list, select the required site.
7. In the Alarm Input Number box, type the alarm input number
8. In the Normal State drop-down list, select Open or Closed as the normal state for the alarm input.
9. From the Operating Mode drop-down list, select the required mode. The available modes are listed in the following table.

Modes	Description
Direct	The alarm condition activates or de-activates when it physically changes state, or is set or cleared with macros.
Latched	Once the alarm is triggered, it remains active until it is reset manually using the alarm clear option.
Toggle	The first time the alarm is triggered it becomes active, the next time it is cleared.

10. In the Connected To section, click one of the devices for which you want to add the alarm input. The following table lists the available devices to which an Alarm Input can be connected.

Device	Description
Switcher	For details on connecting a switcher, see Connecting Alarm Input to the Switcher .
Recorder	For details on connecting a recorder, see Connecting Alarm Input to the Recorder .
Remote Camera	For details on connecting a remote camera, see Connecting Alarm Input to the Remote Camera .
Keyboard	For details on connecting a keyboard, see Connecting Alarm Input to the Keyboard .
Network	For details on connecting a network, see Connecting Alarm input to the Network .
High Level Device	For details on connecting a high level device, see Connecting Alarm Input to the High Level Device .

11. Select the LINK check box if you want to broadcast the status changes and actions performed on the current alarm input on the network.
12. Associate Partition.
13. Click Save.

Note: You can switch on or switch off an alarm input using the On and Off buttons under Trigger Alarm Input.

Connecting Alarm input to the Network

To connect alarm input to a network

1. In the Network box, type the network node and the video input device number for which you want to associate the alarm input.
2. On the Event Settings tab, specify the following details.

Settings	Description
Event Description	Type a description for the event.
Start Macro	Type an alarm start macro. When an alarm condition is detected for an alarm input, the alarm start macro is executed.
Finish Macro	Type an alarm finish macro. When a detected alarm input returns to its normal state, the alarm finish macro is executed.
Global ID	Type a unique global ID. If the Global Event ID is not assigned, MAXPRO VMS assigns a unique global ID automatically when you save the event settings.
Severity	Type a severity level. Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

3. On the Event Groups tab, select the check box corresponding to the event group that you want to associate to the alarm input, and then click Associate.
4. Click Save.

Connecting Alarm Input to the Recorder

To connect alarm input to a recorder

1. From the Recorder drop-down list, select the required recorder. The recorder settings appear.
2. In the Alarm Input ID text box under Input Settings tab, type the Alarm Input ID.
3. On the Event Settings tab, specify the following details.

Settings	Description
Event Description	Type a description for the event.
Start Macro	Type an alarm start macro. When an alarm condition is detected for an alarm input, the alarm start macro is executed.
Finish Macro	Type an alarm finish macro. When a detected alarm input returns to its normal state, the alarm finish macro is executed.

Settings	Description
Global ID	Type a unique global ID. If the Global Event ID is not assigned, MAXPRO VMS assigns a unique global ID automatically when you save the event settings.
Severity	Type a severity level. Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

- On the Event Groups tab, select the check box corresponding to the event group that you want to associate to the alarm input, and then click Associate.
- Click Save.
- For connecting alarm input to a Enterprise, see [Connecting to Enterprise](#).

Connecting to Enterprise

- On the Input Settings tab, specify the following details.

Site ID	Type the site ID of the recorder.
Station ID	Type the station ID of the recorder.
Bit Filter Type	Type the bit filter type
Bit Filter ID	Type the bit filter ID.
Source Information	The source information is automatically updated when the Discover Cameras feature is used.

- On the Event Settings tab, specify the following details.

Settings	Description
Event Description	Type a description for the event.
Start Macro	Type the required macro to start the event. When an alarm condition is detected for an alarm input, the alarm start macro is executed.
Finish Macro	Type the required macro to end the event. When a detected alarm input returns to its normal state, the alarm end macro is executed.
Global ID	Type a unique global ID. If the Global Event ID is not assigned, MAXPRO VMS assigns a unique global ID automatically when you save the event settings.

Settings	Description
Severity	Type a severity level. Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

Connecting Alarm Input to the Remote Camera

To connect alarm input to a remote camera

1. From the Remote Camera drop-down list, select the required camera. The remote camera settings appear.
2. On the Event Settings tab, specify the following details.

Settings	Description
Event Description	Type a description for the event.
Start Macro	Type an alarm start macro. When an alarm condition is detected for an alarm input, the alarm start macro is executed.
Finish Macro	Type an alarm finish macro. When a detected alarm input returns to its normal state, the alarm finish macro is executed.
Global ID	Type a unique global ID. If the Global Event ID is not assigned, MAXPRO VMS assigns a unique global ID automatically when you save the event settings.
Severity	Type a severity level. Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

3. On the Event Groups tab, select the check box corresponding to the event group that you want to associate to the alarm input, and then click Associate.
4. Click Save.

Connecting Alarm Input to the Switcher

To connect alarm input to a switcher

1. From the Switcher drop-down list, select the required switcher. The switcher settings appear.
2. On the Advanced Settings tab, specify the following details.
3. On the Event Settings tab, specify the following details.
4. On the Event Groups tab, select the check box corresponding to the event group that you want to associate to the alarm input, and then click Associate.
5. Click Save.

Settings	Description
Subrack ID	Specifies the subrack ID number where the alarm input module resides. The valid range is 1 – 99. If a high level or mimic panel alarm is used, the number is prefixed with an “H”. If a keyboard alarm is used, the number is prefixed with a “K”. For VideoBlox Subrack, this ID represents the ‘V’+communication port number to which the VideoBlox alarm concentrator AVBPIT is connected. Valid range is ‘V’+maximum communication ports.
Subrack Slot	This field defines the slot number within the control subrack where the alarm input module resides. Valid slot numbers are 1 – 32 for I/O and combination video/I/O subracks, and 15 – 17 for HD Series subracks. For VideoBlox Subrack, this number represents the alarm concentrator AVBPIT number. Valid range is 0 to 255.

Settings	Description
Event Description	Type a description for the event.
Start Macro	Type an alarm start macro. When an alarm condition is detected for an alarm input, the alarm start macro is executed.
Finish Macro	Type an alarm finish macro. When a detected alarm input returns to its normal state, the alarm finish macro is executed.
Global ID	Type a unique global ID. If the Global Event ID is not assigned, MAXPRO VMS assigns a unique global ID automatically when you save the event settings.
Severity	Type a severity level. Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

Connecting Alarm Input to the High Level Device

To connect alarm input to a high level device

1. In the High Level Device box, type the device number.
2. On the Advanced Settings tab, specify the following details

Settings	Description
Subrack ID	The Subrack ID number where the alarm input resides is displayed automatically. The valid range is 1 – 99. If a high level or mimic panel output is used, the number is prefixed with an “H”. If a keyboard output is used, the number is prefixed with a “K”. For VideoBlox subrack, this represents the ‘V’+communication port number to which the VideoBlox alarm concentrator AVBPIT is connected. Valid range: ‘V’+maximum communication ports.
Subrack Slot	Type a slot number within the control subrack where the alarm input resides.

3. On the Event Settings tab, specify the following details.

Settings	Description
Event Description	Type a description for the event.
Start Macro	Type an alarm start macro. When an alarm condition is detected for an alarm input, the alarm start macro is executed.
Finish Macro	Type an alarm finish macro. When a detected alarm input returns to its normal state, the alarm finish macro is executed.
Global ID	Type a unique global ID. If the Global Event ID is not assigned, MAXPRO VMS assigns a unique global ID automatically when you save the event settings.
Severity	Type a severity level. Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

4. On the Event Groups tab, select the check box corresponding to the event group that you want to associate to the alarm input, and then click Associate.
5. Click Save.

Connecting Alarm Input to the Keyboard

To connect alarm input to a keyboard

1. From the keyboard drop-down list, select the required joystick controller. The keyboard settings appear.
2. On the Advanced Settings tab, specify the following details.

Settings	Description
Subrack ID	The Subrack ID number where the alarm input resides is displayed automatically. The valid range is 1 – 99. If a high level or mimic panel output is used, the number is prefixed with an “H”. If a keyboard output is used, the number is prefixed with a “K”. For VideoBlox subrack, this represents the ‘V’+communication port number to which the VideoBlox alarm concentrator AVBPIT is connected. Valid range: ‘V’+maximum communication ports.
Subrack Slot	Type a slot number within the control subrack where the alarm input resides.

3. On the Event Settings tab, specify the following details.

Settings	Description
Event Description	Type a description for the event.

Settings	Description
Start Macro	Type an alarm start macro. When an alarm condition is detected for an alarm input, the alarm start macro is executed.
Finish Macro	Type an alarm finish macro. When a detected alarm input returns to its normal state, the alarm finish macro is executed.
Global ID	Type a unique global ID. If the Global Event ID is not assigned, MAXPRO VMS assigns a unique global ID automatically when you save the event settings.
Severity	Type a severity level. Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

4. On the Event Groups tab, select the check box corresponding to the event group that you want to associate to the alarm input, and then click Associate.
5. Click Save.

Associating Partitions to the Alarm Input

You can associate partition to alarm inputs. Associating a partition to an Alarm Input restricts a non - associated user from viewing or modifying the Alarm Input.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partitions to alarm input

1. Click the Partitions tab. The screen displays the associated partitions, if any.
2. Click Associate. The Select Partitions page appears.
3. Select the check box corresponding to the partition name you want to associate.
4. Click OK. The selected partition is displayed in the list of associated partitions.

To disassociate partitions from alarm input

- Select the check box corresponding to the partition name, and then click Remove.

Deleting the Alarm Input

You can delete an alarm input when you do not want external device to raise an alarm. All the associations made to the alarm inputs are removed, when you delete it.

Before you begin

- Disassociate Partitions. [Associating Partitions to the Alarm Input](#) for more information.

To delete alarm input

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Alarm Inputs. The Alarm Input screen appears in the display area.
3. Select the check box corresponding to the alarm inputs that you want to delete.
4. Click Delete. A confirmation message appears on the top of the display area.
5. Click Yes.

Updating the Alarm Input

You can update alarm input to change its association with a partition and also to modify its settings.

To update alarm input

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Alarm Inputs. The Alarm Input screen appears in the display area.
3. Select the check box corresponding to the alarm input you want to update.
4. Click Update. The settings for the alarm input appear. You can modify the settings.

Contact Group

Contact group is a group of users in MAXPRO VMS. You can create contact groups of users with different roles. For example, you can create a contact group of users who are associated to operator role. Alarm notifications can be sent to a contact group.

Adding a Contact Group

You can add a user group to group the users on the basis of the roles. Only the “admin” user can add a contact group in MAXPRO VMS.

Before you begin

- Add Roles. See [Adding a role](#) for more information.
- Add Users. See [Adding a User](#) for more information.
- Add Workstations. [Adding a Workstation](#) for more information.
- Add Partition. See [Adding a Partition](#) for more information.

To add a contact group

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Contact Group. The Contact Group screen appears in the display area.

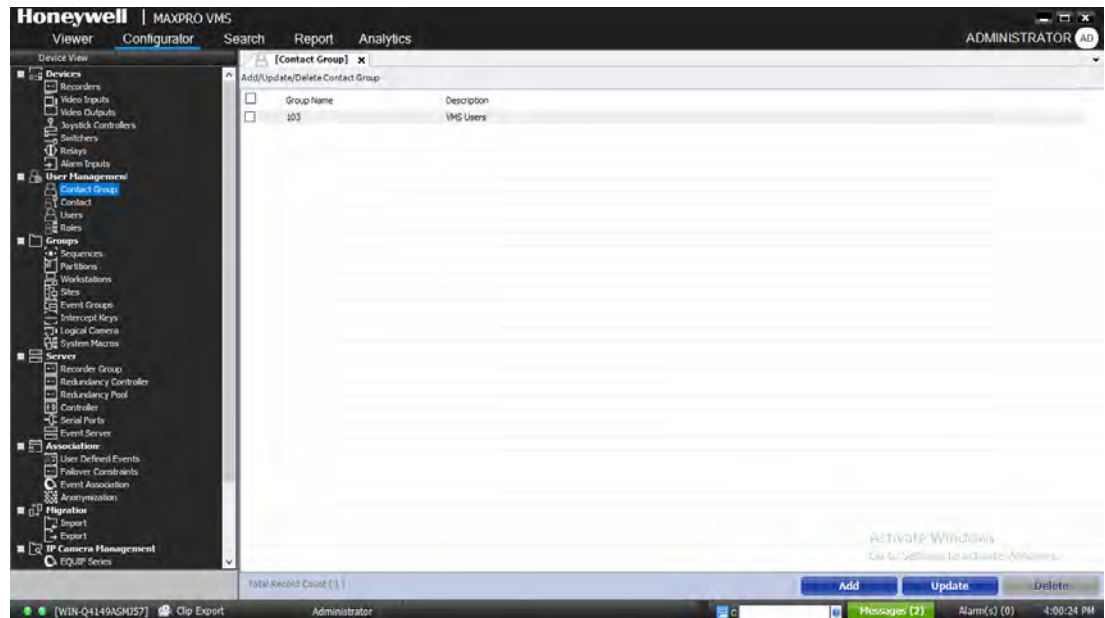


Figure 4-38 Contact Group

3. Click Add. The settings for the contact group appears.

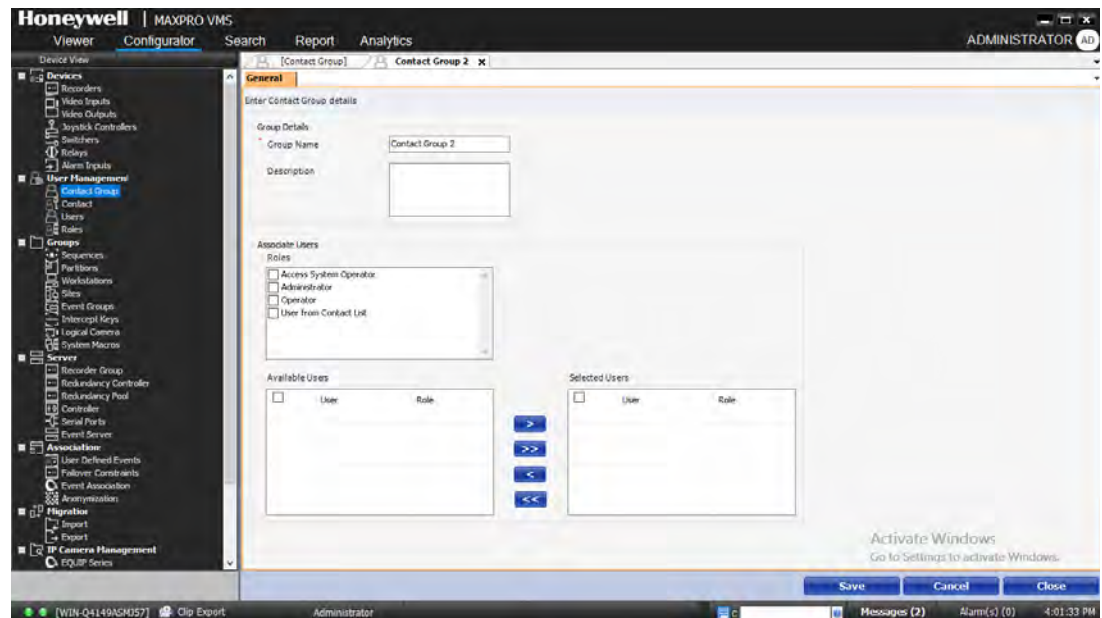






Figure 4-39 Adding a Contact Group

4. In the Group Name box, type the name for the group.
5. In the Description box, type a description for the contact group.
6. In the Associate Users section, select the required role. The users associated to the role are displayed in the Available Users section.

7. In the Available Users section, select the check box corresponding to the user whom you want to select, and then click  or click  to select all the users. Similarly, select to deselect  or  to deselect all.
8. Click Save.

Deleting the Contact Group

You can delete a contact group when you no longer want to keep the contact group.

To delete a contact group

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Contact Group. The Contact Group screen appears in the display area.
3. Select the check box corresponding to the contact group that you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Updating the Contact group

You can update a contact group to change the users and roles for a contact group.

To update a contact group

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Contact Group. The Contact Group screen appears in the display area.
3. Select the check box corresponding to the contact group you want to update.
4. Click Update. The settings for the contact group appear. You can modify the settings.

Contacts

Adding a contact

You can add and store a contact in MAXPRO VMS. Only an user with administrator privileges can add contacts.

To add a contact

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Contact. The Contact screen appears in the display area.

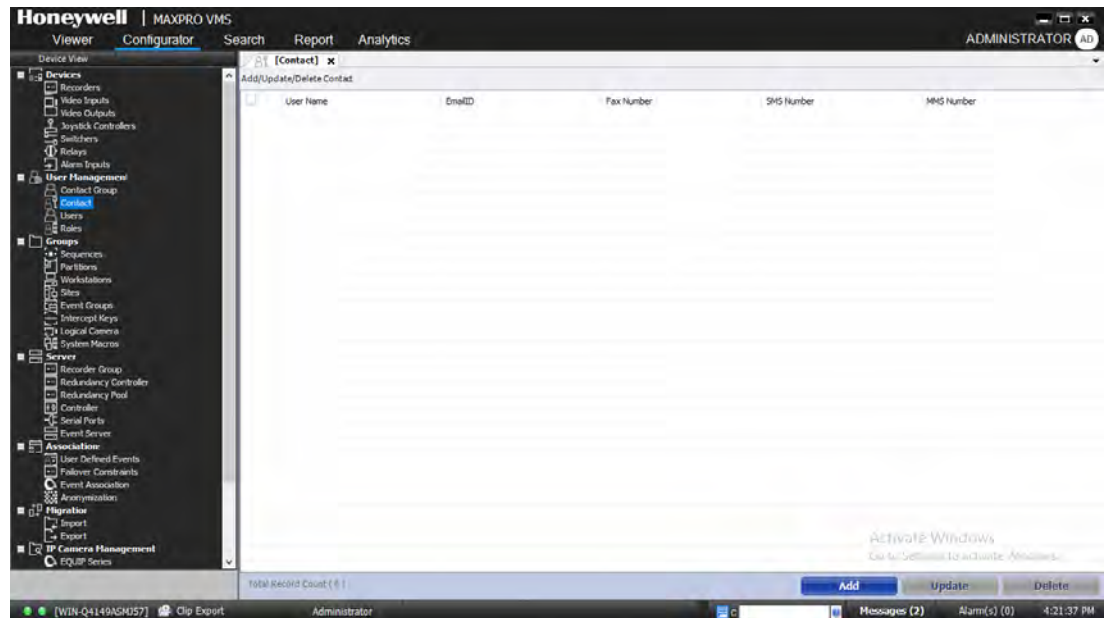


Figure 4-40 Contact

3. Click Add. The general settings for the contact appears.

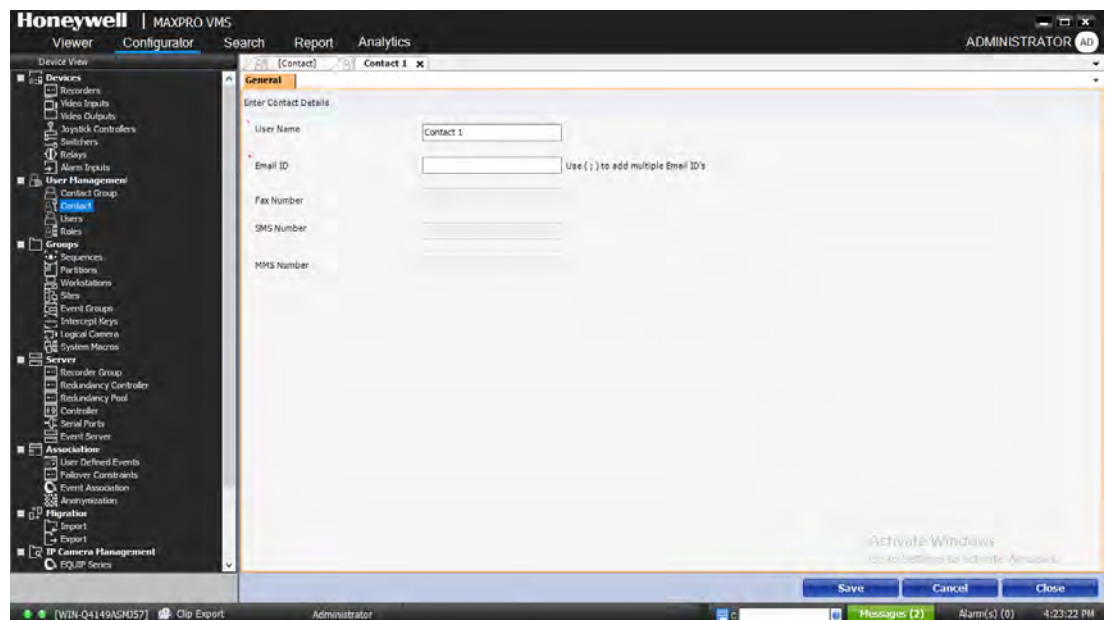


Figure 4-41 Adding a Contact

4. In the User Name box, type a name for the user.
5. In the Email ID box, type the email ID for the user, if required.
6. Click Save.

Users

A user in MAXPRO VMS 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 VMS —System Local User and Windows User. Any new user when added is automatically associated to all the event groups and joystick controller. You can remove the association of a user to event groups and joystick controller to limit the access.

System Local User

A system local user can access only MAXPRO VMS. This user may not have the access to client workstation.

Windows User

A windows user can access client workstation and also MAXPRO VMS.

Users and Roles

Roles are provided to a user. These roles comprise in them 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 “admin” User

The first time MAXPRO VMS is deployed at a site, a default user named “admin” is created. The “admin” user is assigned the role “administrator”. Only this user can add new users, assign roles to the added users, add or modify the privileges to the users, and also assign the users to partitions.

Users and Partitions

A partition is a logical grouping of video devices. Partitions are associated to users. Users are directly associated to the partition which is associated to the role. Users can view and manage the video devices that are grouped inside the associated partitions. A user can also be associated to other partitions which are not associated to the assigned role.

Users and Joystick controllers

Joystick controllers are keyboards that are attached to video outputs in MAXPRO VMS. Users are associated to joystick controllers. These users can use the associated joystick controllers to carry the video surveillance tasks in MAXPRO VMS.

Users and Event Groups

An event group is a set of events that occur on video devices. Users are associated to Event Groups. When any event in the event group occurs, only the users who are associated to the event group can acknowledge the event.

Users and Workstations

A workstation is a computer in which the MAXPRO VMS user interface is installed. Workstations are associated to Users. Users associated to a workstation can log on to MAXPRO VMS user interface and perform various actions. Users are directly associated to the workstation which is associated to the role. A user can be associated to other workstations also which are not associated to a role.

Adding a User

You can add a user by providing a unique user name and a password.

Only “admin” can add a new user in MAXPRO VMS.

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

Note: Honeywell recommends you to change the default Password before you logon to MAXPRO VMS. Refer to [Securing MAXPRO® VMS Technical Notes](#) for further details

After you add a new user, you can assign a role to it. After the role is assigned to the user, the privileges that are defined as a part of the role are also added to the user. You can add or remove any privileges for the specific user-role combination using the “Customized Privileges” option.

Before you begin

- Add Role. See [Adding a role](#) for more information.

By default, a partition and a workstation are available. You can associate a user to them or create new.

To add a user

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Users. The Users screen appears in the display area.

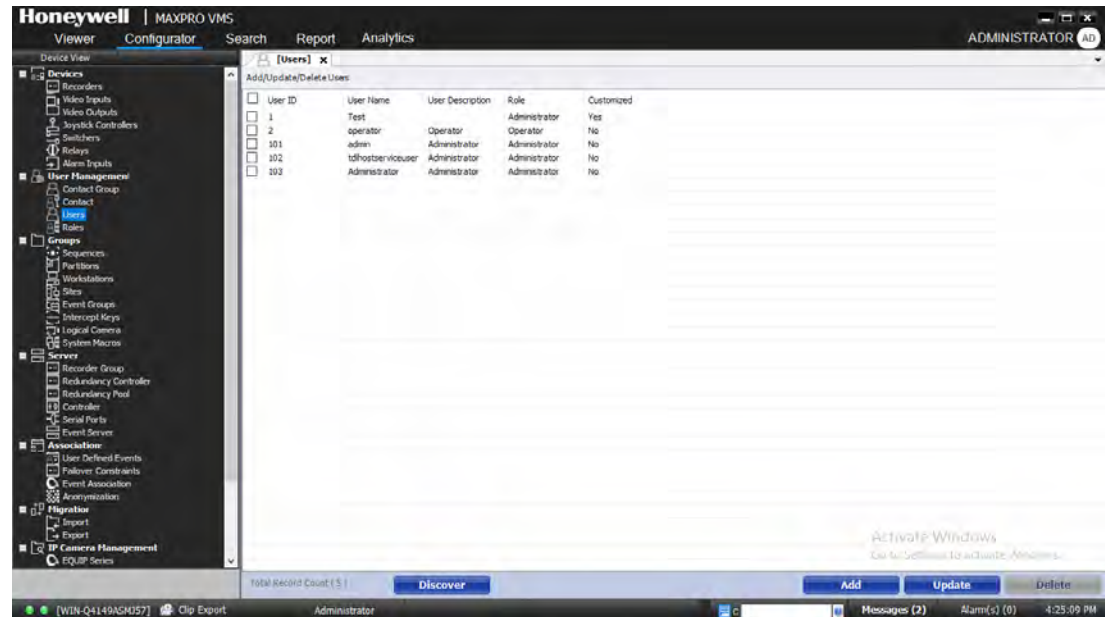


Figure 4-42 Users

3. Click Add. The General Settings tab appears.

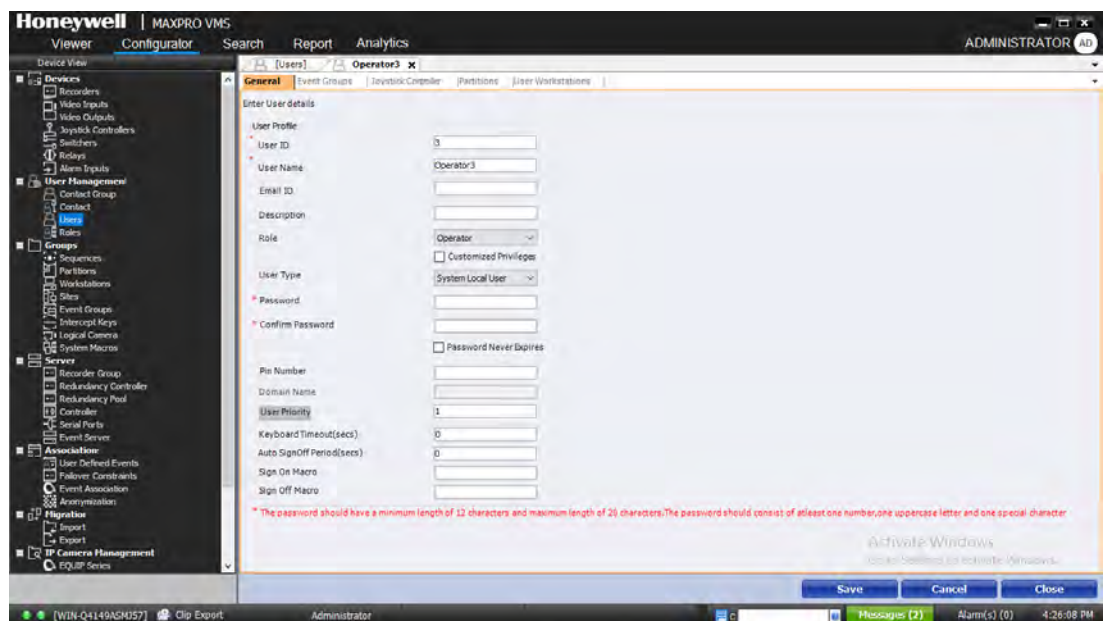


Figure 4-43 Adding User

4. In the User ID box, type a name for the user.
5. In the User Name box, type the name of the user.
6. In the Description box, type the required description.

7. In the Role box, select the role you want to assign to the user.
8. Select the Customized Privileges check box to enable or disable privileges for a user. The following table lists the privileges you can enable for a user.

Privileges	Description
Viewer	
Viewer Access	To restrict access to viewer tab.
Site View	To view sites.
Alarm	To view alarms.
ImageClipTreeView	To view image clip tree.
Message Box	To view message box.
MyDevices	To view MyDevices.
Shared Devices Permission	To view and restrict shared devices.
KeyboardUtility	To access virtual keyboard.
Store Pre-shots	To store pre-shots
Reloading Device Connections	To reload the device connections.
View/Update License	To view or update license.
Iris Access	To access iris of the camera.
Focus Access	To access focus access of the camera.
Monitors	To view monitors.
Sequences	To view sequences.
Salvo Views	To view salvo.
Add My Salvo View	To add my salvo view.
Modify My Salvo View	To modify my salvo view.
Delete My Salvo View	To delete my salvo view.
Add Shared Salvo View	To add shared salvo view.
Modify Shared Salvo View	To modify shared salvo view.
Delete Shared Salvo View	Delete Shared Salvo View.

Privileges	Description
Add or update Surrounding Camera	To add or update surrounding camera.
Enable/Disable Camera	To enable or disable the cameras.
Configure Privacy	To configure the privacy settings.
Show Calender Search	To display the calender search.
Show Profile Camera	To display profile camera
Change Password	To change password
Show Global Bookmarks	To display global bookmarks
Four Eye Authentication	To enable the Four Eye Authentication feature
Hide Subject Identity	To enable the Hide subject Identity option
Time Line	
TimeLine Access	To allow the user to access TimeLine window.
Clip Delete	To delete video clips.
Image Delete	To delete images.
Create Bookmark	To create bookmark.
View Bookmark	To view bookmark.
Delete Bookmark	To delete bookmark.
Create Loop	To allow user to create loop.
Update loop	To allow user to update loop.
Clip Creation	To allow user to create clips.
Configurator	
Configurator Access	To allow user to access configurator.
Add Switcher	To allow user to add switcher.
Update Switcher	To allow user to update switcher.
Delete Switcher	To allow user to delete switcher.
Add System Macro	To allow user to add system macro.
Update System Macro	To allow user to update system macro.

Privileges	Description
Delete System Macro	To allow user to delete system macro.
Add Logical Camera	To allow user to add logical camera.
Update Logical Camera	To allow user to update logical camera
Delete Logical Camera	To allow user to delete logical camera
Add Relay	To add relay.
Update Relay	To update relay.
Delete Relay	To delete relay.
Add Alarm Input	To add an alarm input.
Update Alarm Input	To update an alarm input.
Delete Alarm Input	To delete an alarm input.
Update Controller	To update controller.
Import	To Import files into MAXPRO VMS.
Export	To export the MAXPRO VMS files.
Configure Equip Camera	To configure equip camera.
Cold/Warm Boot	To allow user to boot.
Add Job	To add a job.
Update Job	To update a job.
Delete Job	To delete a job.
Add Contact	To add a contact.
Update Contact	To update a contact.
Delete Contact	To delete a contact.
Add Contact Group	To add a contact group.
Update Contact Group	To update a contact group.
Delete Contact Group	To delete a contact group.
Add User	To add new users.
Delete User	To allow user to delete new users.
Modify User Privilege	To modify user privilege.

Privileges	Description
Add Recorder	To allow user to add recorder.
Update Recorder	To allow user to update recorder.
Delete Recorder	To allow user to delete recorder.
Add Video Input	To allow user to add Video Input.
Update Video Input	To allow user to update video input.
Delete Video Input	To allow user to delete video input.
Add Video Output	To allow user to add video output.
Update Video Output	To allow user to update video output.
Delete Video Output	To allow user to delete video output.
Add Sequence	To allow user to add sequence.
Update Sequence	To allow user to update sequence.
Delete Sequence	To allow user to delete sequence.
Add Port	To allow user to add a port.
Update Port	To allow user to update a port.
Delete Port	To allow user to delete a port.
Add Partition	To allow user to add a partition.
Update Partition	To allow user to update a partition.
Delete Partition	To allow user to delete a partition.
Add Site	To allow user to add a site.
Update Site	To allow user to update a site.
Delete Site	To allow user to delete a site.
Add Workstation	To allow user to add a workstation.
Update Workstation	To allow user to update a workstation.
Delete Workstation	To allow user to delete a workstation.
Add Event Group	To allow user to add event group.
Update Event Group	To allow user to update event group.
Delete Event Group	To allow user to delete event group.
Add Intercept	To allow user to add intercept keys.
Update Intercept	To allow user to update joystick controller.
Delete Intercept	To allow user to delete intercept

Privileges	Description
Update Joystick Controller	To allow user to update joystick controller
Add Role	To allow user to add role.
Update Role	To allow user to update role.
Delete Role	To allow user to delete role.
Immervision	To add Immervision
Failover	To add Failover
Anonymization	To allow user to use/configure Anonymization feature
Search	
Search Access	To allow user to access search features.
Clip Archive	To allow user to perform clip archive.
Clip Restore	To allow user to perform clip restore.
Clip Delete	To allow user to perform to delete clip.
Reports	
Report Access	To allow user to access report features.
Saved Reports	To allow user to access saved reports
Controller Operator Privileges	
Display Name	To display the users name.
Multiple SignOn	To allow user to be signed on to more than one keyboard at a time.
Swap PTZ Up Down	To reverse the up/down control of a pan/tilt camera when it is being used by user.
Scan Set	To allow user to edit scan sequences.
Camera View Set	To allow user to set PTZ camera views.
UserMacro Set	To allow user to create user keyboard macros
Camera Analog PTZ	To allow user to set PTZ options for analog camera.
Standard Device	To allow user to control standard device functions.
Video Recorder	To allow user to control VCR functions.
Smart Device	To allow user to control smart device functions.
Controller Menu Access	
Video Disable	To disable live video view for a user.
ScanSequence Lock Unlock	To allow user to lock or unlock scan sequences.

Privileges	Description
VideoControl Lock Unlock	To allow user to lock or unlock video control.
Set Clock	To allow user to set the system time and date.
SignOff	To allow user to sign off from a key board.
Change Pin	To allow user to change the PIN of all system users.
Status Information	To allow user to change the current system status.
Alarm Enable Disable	To allow system user to enable or disable system alarms.
System Configuration	To allow user to run the Windows SetMax configuration editor, save the current system environment as the default settings, or exit to Windows.
UserMacro Lock Unlock	To allow user to lock or unlock user macros.
ToolBar Buttons	
SalvoLayouts...1, 4, 6, 9,10,13,16	To allow user to add or access different salvolayouts.
Surrounding Camera	To allow user to view surrounding cameras.
Full Screen Mode	To allow user to view full screen mode.
Sync PlayBack Mode	To allow user to access the sync playback mode.
Remote Monitor Mode	To allow user to access the remote monitor mode.
Incident management Mode	To allow user to access the incident management mode.
Create Salvo	To allow user to create a salvo.
Application Launch Pad	To allow user to access the application launch pad.
Salvo Snapshot	To allow user to capture a salvo snapshot.
Instant Clip Export	to enable user to instantly export a clip.
Snapshot	To capture a snapshot.
Color Correction	Allow user to perform color correction
Flip	Allow user to flip a video
Mirror	Allow user to mirror view a video
Preview	Allow user to preview a video

Privileges	Description
Remove Text Overlay	Allow user to remove text overlay
Analytics	
Add Analytics server	To add analytics server
Update Analytics server	To update analytics server
Delete Analytics server	To delete analytics server
Launch HVA Configurator	To launch HVA configurator
Launch HVA Live Monitor	To launch HVA Live Monitor
Reports and Forensics	To access the reports and forensics
Enable Analytics Option for Camera	To allow user to enable the analytics option for camera

Note: To enable all the privileges select the *Allow All* check box and to deny all the privileges, select the *Deny All* check box.

9. From the User Type drop-down list, select System Local User or Windows User.
10. In the Password box, type the configured user password.
11. In the Confirm Password box, retype the user password.
12. In the Pin Number box, type the Pin number. The Pin number is required only for Ultrakey keyboard and not required for MAXPRO VMS client login.
13. In the Domain Name box, type the name of the domain. Currently this box is disabled.
14. In the Keyboard Timeout (Sec) box, type the time out value.
15. In the Auto SignOff Period (Sec) box, type the time out value.
16. In the Sign On Macro box, type the sign on macro.
17. In the Sign Off Macro box, type the sign off macro.
18. Associate Partitions. See [Associating Partitions to the User](#) for more information.
19. Associate Joystick Controllers. See [Associating joystick controller to users](#) for more information.
20. Associate Event Groups. See [Associating Event Groups to Users](#) for more information.
21. Associate Workstations. [Associating Workstations to the Users](#) for more information.
22. Click Save.

Associating Partitions to the User

You can associate partitions to a user. Associating partitions to a user enables the user to perform video surveillance tasks for all the video devices that are grouped in the partition.

You can associate more than one partition to a user.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partitions to a user

1. Click the Partitions tab. The screen displays the associated partitions, if any.

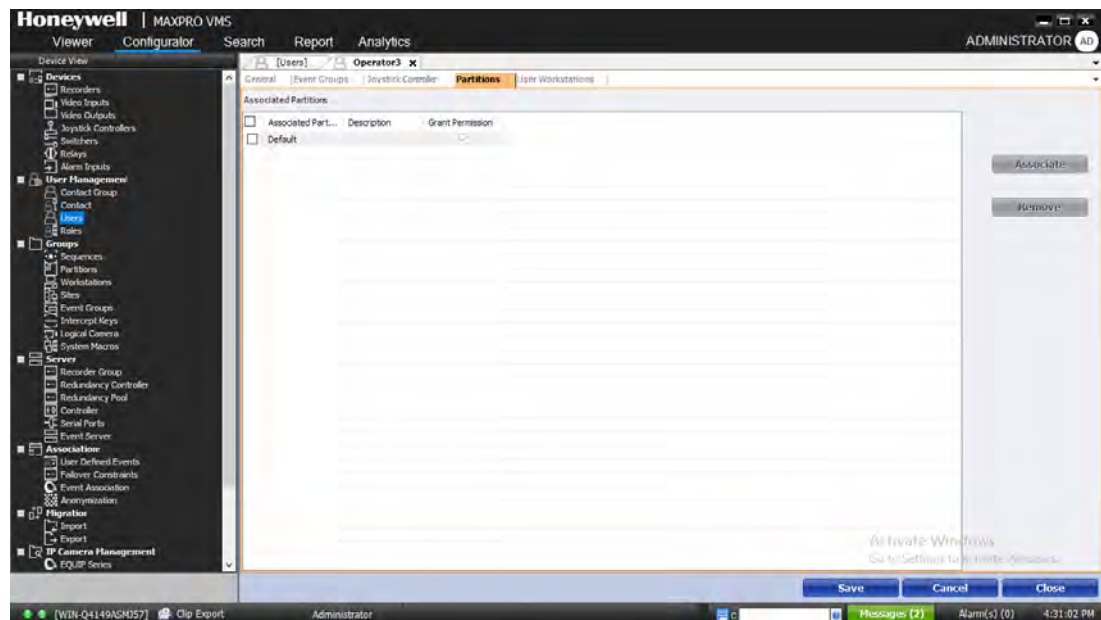


Figure 4-44 User Partitions

2. Click Associate. The Select Partitions page appears.
3. Select the check box corresponding to the partition name you want to associate.
4. Click OK.

To disassociate partitions from a user

- Select the check box corresponding to the partition name, and then click Remove.

Associating Workstations to the Users

You can associate workstations to users to log on to MAXPRO VMS user interface and perform various actions.

Before you begin

- Add a Workstation. [Adding a Workstation](#) for more information.

To associate a user to workstation

1. Click the User Workstations tab. The screen displays the associated workstations if any.

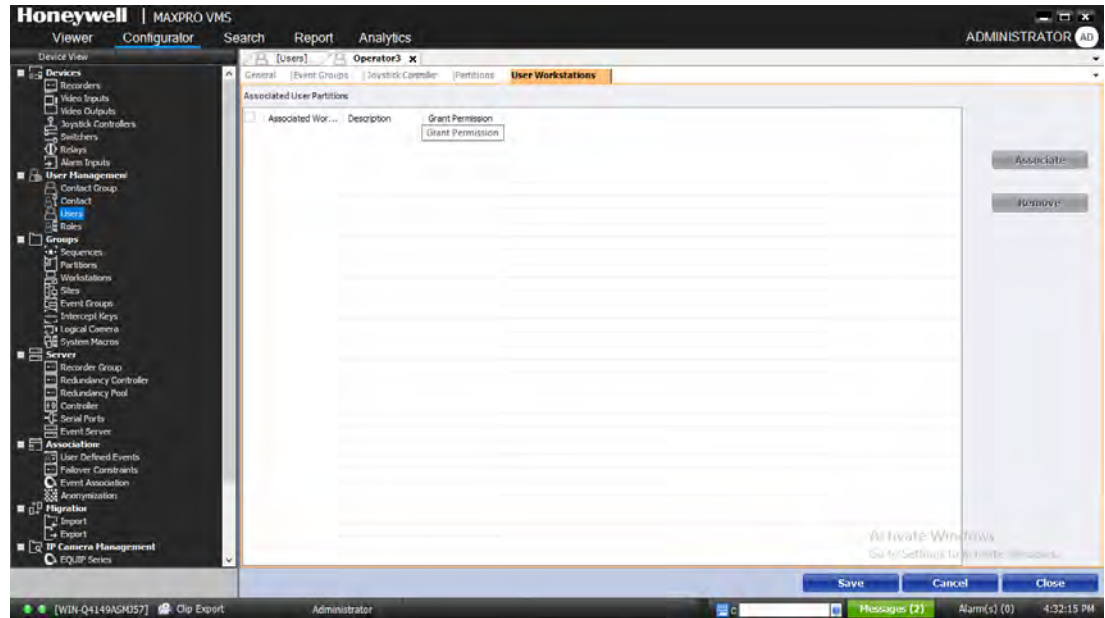


Figure 4-45 User Workstations

2. Click Associate. The Select User Workstation page appears.
3. Select the check box corresponding to the workstation name you want to associate.
4. Click OK.

To disassociate workstation from a user

- Select the check box corresponding to the workstation name, and then click Remove.

Associating joystick controller to users

You can associate users to joystick controllers to perform video surveillance tasks in MAXPRO VMS.

Before you begin

- Add a joystick controller.

To associate the joystick controller to a user

1. Click the Joystick Controller tab. The screen displays the associated joysticks if any.

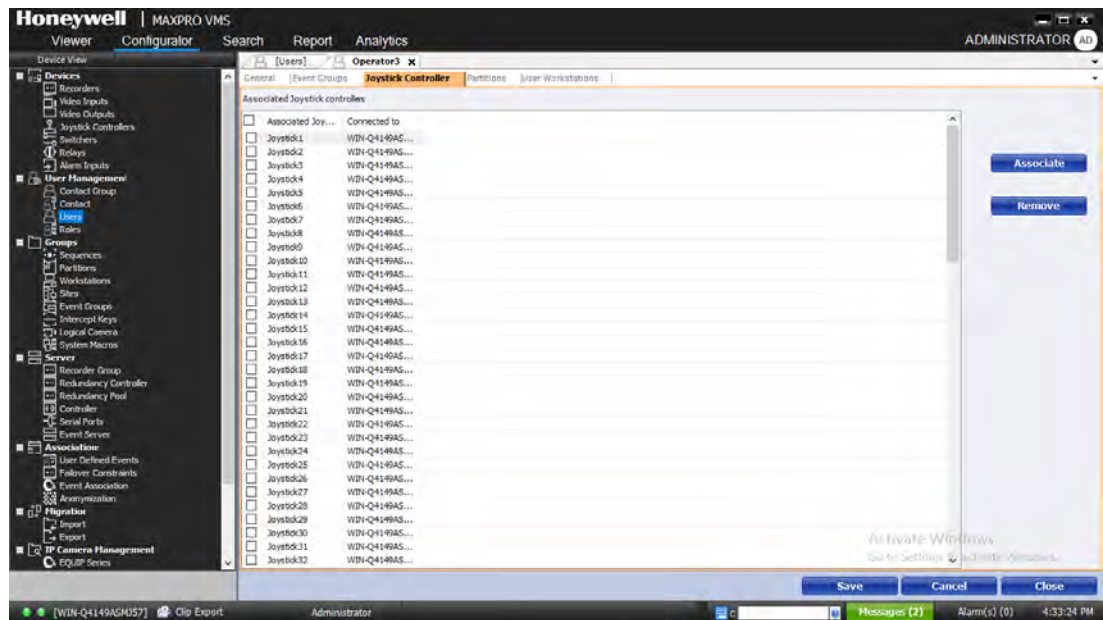


Figure 4-46 User Joystick Controller

2. Click Associate. The Select Joystick Controller page appears.
3. Select the check box corresponding to the joystick name you want to associate.
4. Click OK.

By default, all the joystick controllers are associated when a user is added. You can remove the joystick controllers that you do not require.

To disassociate Joystick Controller from user

- Select the check box corresponding to the joystick name, and then click Remove.

Associating Event Groups to Users

You can associate a user to a event group to acknowledge the event that occurs in it.

Before you begin

- Add Event Group.

To associate a event group to a user

1. Click the Event Groups tab. The screen displays the associated event groups if any.

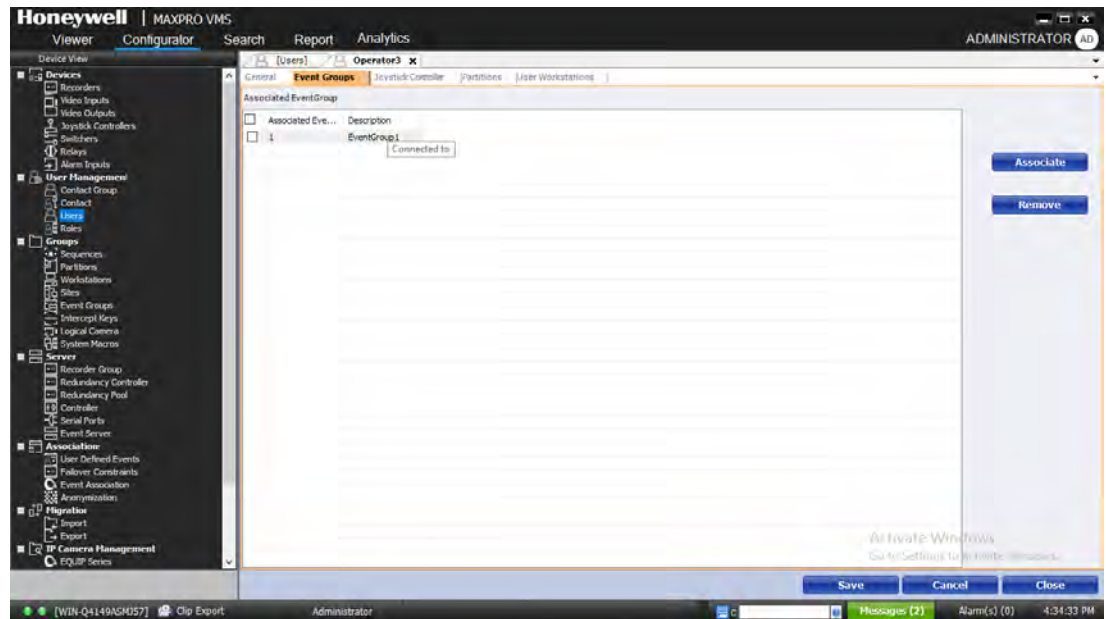


Figure 4-47 User Event Groups

2. Click Associate. The Select Event Groups page appears.
3. Select the check box corresponding to the Event Group name you want to associate.
4. Click OK.

To disassociate event group from a user

- Select the check box corresponding to the Event Group name, and then click Remove.

Discovering and Importing Users

You can discover users connected to a domain or workstation and add them to the MAXPRO VMS.

To discover and import users

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Users. The Users screen appears in the display area.
3. Click Discover. The User Discovery Details screen appears.
4. In the Domain/Workgroup drop-down list, select the domain or workgroup.

5. In the Name Filter box, type the name which you want to discover.

Note: *If you want to search more than one name belonging to the same category, type the full name or partial name succeeded by a “*”, and then click Query. For example, to search users who have their first name as John, type John* or Joh*, and then click Query.*

6. Click Query. The results are displayed in the Results section. The users who are not added to MAXPRO VMS are listed in green color.
7. Select the check box corresponding to the required user.
8. In the User Role drop-down list, select a role for the user.
9. Click Import. The user is added and his name is listed in red color.

Note: *You can skip step 5 if you do not want to use name filter option.*

10. Click Reset to restore default settings or to discover new users.

Updating a User

You can modify the settings of user to change the user ID, password and enable privileges. You can update user settings only if you have admin rights.

To update a user

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Users. The Users screen appears in the display area.
3. Select the check box corresponding to the user.
4. Click Update. The general settings for the user appear. You can modify the settings.

Deleting a user

You can remove a user from MAXPRO VMS. When you delete a user, all the associations made to the user are also removed.

To delete a user

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Users. The Users screen appears in the display area.
3. Select the check box corresponding to the user you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Roles

The users in MAXPRO VMS perform various video surveillance operations. The surveillance operations can be monitoring the live video, recording scenes of interest and so on. Some of these operations can be critical while some can be routine ones that are performed every day.

A user can be responsible for carrying out the routine tasks or critical tasks. This responsibility for performing various tasks is provided to the users by means of roles. With every role, there are a set of predefined privileges that are also assigned to the user. While a role can be just a label that is assigned to a user, like Operator or Administrator, it is the privileges that provide the right and responsibility for carrying out the operations.

Administrator and operator are the predefined roles in MAXPRO VMS and consists of a set of privileges. The role Administrator cannot be deleted or updated. Apart from the predefined roles, you can add a new role with a set of privileges. When you associate users to the role, the privileges that are defined as a part of the role is also added to the user. Any new partition and workstation added are automatically associated to the administrator role. If required, you can also add or remove privileges for a user-role combination. The modified set of privileges is applied only to the specific user-role combination and does not change the privilege set for the role.

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

Roles and Partitions

A partition is a logical grouping of video devices. Partitions are associated to Roles. Roles are assigned to users, which enable them to view and manage the video devices that are grouped inside the associated partitions.

Roles and Workstations

A workstation is a computer in which the MAXPRO VMS user interface is installed. Workstations are associated to Roles. Roles are assigned to users which enables them to log on to MAXPRO VMS user interface and perform various actions.

Adding a role

You can add a new role by providing a role name. After adding a role, you can associate users to it. The role along with its set of privileges is added to the user.

You can also add or remove privileges to the user-role combination. In addition, you can also deny all privileges to the user-role.

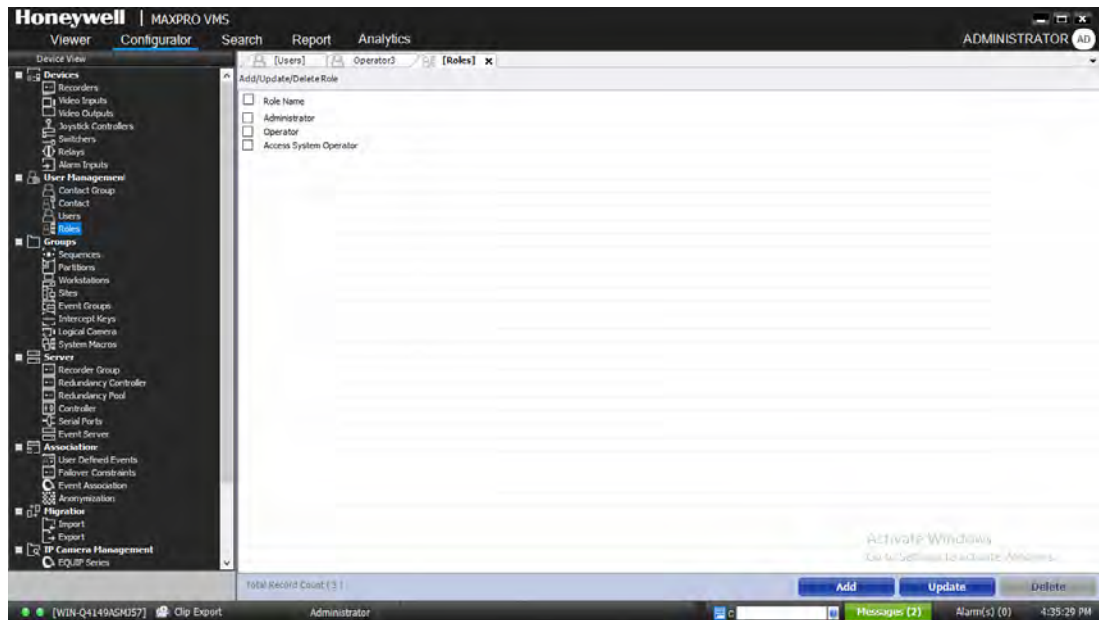
Before you begin

- Add Workstations. See [Adding a Workstation](#) for more information.
- Add Partition. See [Adding a Partition](#) for more information.

By default, a partition and a workstation are available. You can associate a role to them or create new.

To add a role

1. Click the Configurator tab.
2. Expand User Management in the navigation area, and then click Roles. The Roles screen appears in the display area.



3. Click Add. The General Settings tab appears.

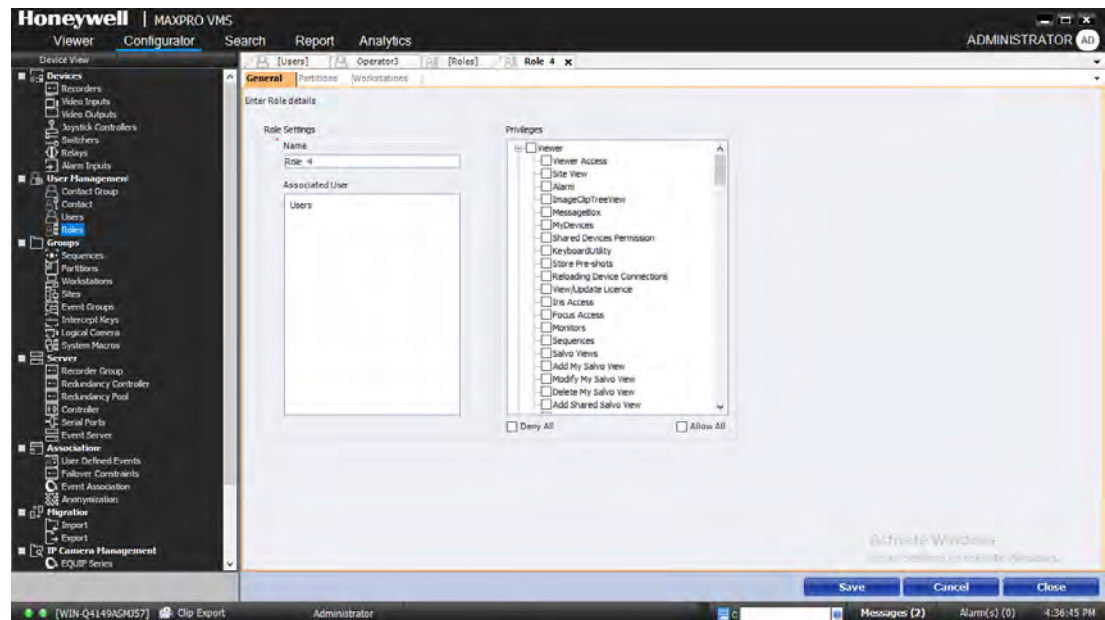


Figure 4-48 Roles General Settings

4. In the Name box, type a name for the role.

5. In the Associated User area, the user associated with the role is displayed.

Note: User is displayed only when the role is associated.

6. In the Privileges section, select the check box corresponding to the privileges for enabling them for the role. The following table lists the privileges you can enable for a user.

Privileges	Description
Viewer	
Viewer Access	To restrict access to viewer tab.
Site View	To view sites.
Alarm	To view alarms.
ImageClipTreeView	To view image clip tree.
Message Box	To view message box.
MyDevices	To view MyDevices.
Shared Devices Permission	To view and restrict shared devices.
KeyboardUtility	To access virtual keyboard.
Store Pre-shots	To store pre-shots
Reloading Device Connections	To reload the device connections.
View/Update License	To view or update license.
Iris Access	To access iris of the camera.
Focus Access	To access focus access of the camera.
Video Outputs	To view Video Outputs.
Monitors	To view/access monitors.
Sequences	To view sequences.
Salvo Views	To view salvo.
Add My Salvo View	To add my salvo view.
Modify My Salvo View	To modify my salvo view.
Delete My Salvo View	To delete my salvo view.
Add Shared Salvo View	To add shared salvo view.
Modify Shared Salvo View	To modify shared salvo view.
Delete Shared Salvo View	Delete Shared Salvo View

Privileges	Description
Add or update Surrounding Camera	To add or update surrounding camera.
Enable / Disable cameras	To allow user to enable/disable cameras.
Configure Privacy	To configure the privacy settings.
Show Calender Search	To display the calender search.
Show Profile Camera	To display profile camera
Change Password	To change password
Show Global Bookmarks	To display global bookmarks
Four Eye Authentication	To enable the Four Eye Authentication feature
Hide Subject Identity	To enable the Hide subject Identity option
Time Line	
TimeLine Access	To allow user to access TimeLine window.
Clip Delete	To delete video clips.
Image Delete	To delete images.
Create Bookmark	To create bookmark.
View Bookmark	To view bookmark.
Delete Bookmark	To delete bookmark.
Create Loop	To allow user to create loop.
Update loop	To allow user to update loop.
Clip Creation	To allow user to create clips.
Configurator	
Configurator Access	To allow user to access configurator.
Add Switcher	To allow user to add switcher.
Update Switcher	To allow user to update switcher.
Delete Switcher	To allow user to delete switcher.
Add System Macro	To allow user to add system macro.
Update System Macro	To allow user to update system macro.
Delete System Macro	To allow user to delete system macro.
Add Logical Camera	To allow user to add logical camera.

Privileges	Description
Update Logical Camera	To allow user to update logical camera
Delete Logical Camera	To allow user to delete logical camera
Add Relay	To add relay.
Update Relay	To update relay.
Delete Relay	To delete relay.
Add Alarm Input	To add an alarm input.
Update Alarm Input	To update an alarm input.
Delete Alarm Input	To delete an alarm input.
Update Controller	To update controller.
Import	To Import files into MAXPRO VMS.
Export	To export the MAXPRO VMS files.
Configure Equip Camera	To configure equip camera.
Cold/Warm Boot	To allow user to boot.
Add Job	To add a job.
Update Job	To update a job.
Delete Job	To delete a job.
Add Contact	To add a contact.
Update Contact	To update a contact.
Delete Contact	To delete a contact.
Add Contact Group	To add a contact group.
Update Contact Group	To update a contact group.
Delete Contact Group	To delete a contact group.
Add User	To add new users.
Delete User	To allow user to delete new users.
Modify User Privilege	To modify user privilege.
Add Recorder	To allow user to add recorder.
Update Recorder	To allow user to update recorder.
Delete Recorder	To allow user to delete recorder.
Add Video Input	To allow user to add Video Input.
Update Video Input	To allow user to update video input.

Privileges	Description
Delete Video Input	To allow user to delete video input.
Add Video Output	To allow user to add video output.
Update Video Output	To allow user to update video output.
Delete Video Output	To allow user to delete video output.
Add Sequence	To allow user to add sequence.
Update Sequence	To allow user to update sequence.
Delete Sequence	To allow user to delete sequence.
Add Port	To allow user to add a port.
Update Port	To allow user to update a port.
Delete Port	To allow user to delete a port.
Add Partition	To allow user to add a partition.
Update Partition	To allow user to update a partition.
Delete Partition	To allow user to delete a partition.
Add Site	To allow user to add a site.
Update Site	To allow user to update a site.
Delete Site	To allow user to delete a site.
Add Workstation	To allow user to add a workstation.
Update Workstation	To allow user to update a workstation.
Delete Workstation	To allow user to delete a workstation.
Add Event Group	To allow user to add event group.
Update Event Group	To allow user to update event group.
Delete Event Group	To allow user to delete event group.
Add Intercept	To allow user to add intercept keys.
Update Intercept	To allow user to update joystick controller.
Delete Intercept	To allow user to delete intercept.
Add Role	To allow user to add role.
Update Role	To allow user to update role.
Delete Role	To allow user to delete role.
Failover	To allow user to perform Failover
Anonymization	To allow user to use Anonymization feature
Search	

Privileges	Description
Search Access	To allow user to access search features.
Clip Archive	To allow user to perform clip archive.
Clip Restore	To allow user to perform clip restore.
Clip Delete	To allow user to perform to delete clip.
Reports	
Report Access	To allow user to access report features.
Saved Reports	To allow user to access saved report.
Controller Operator Privileges	
Display Name	To display the users name.
Multiple SignOn	To allow user to be signed on to more than one keyboard at a time.
Swap PTZ UpDown	To reverse the up/down control of a pan/tilt camera when it is being used by user.
Scan Set	To allow user to edit scan sequences.
Camera View Set	To allow user to set PTZ camera views.
UserMacro Set	To allow user to create user keyboard macros
Camera Analog PTZ	To allow user to set PTZ options for analog camera.
Standard Device	To allow user to control standard device functions.
Video Recorder	To allow user to control VCR functions.
Smart Device	To allow user to control smart device functions.
Controller Menu Access	
Video Disable	To disable live video view for a user.
ScanSequence Lock Unlock	To allow user to lock or unlock scan sequences.
VideoControl Lock Unlock	To allow user to lock or unlock video control.
VideoSource Lock Unlock	To allow user to lock or unlock videosource.
Set Clock	To allow user to set the system time and date.
SignOff	To allow user to sign off from a key board.
Change Pin	To allow user to change the PIN of all system users.
Status Information	To allow user to change the current system status.
Alarm Enable Disable	To allow system user to enable or disable system alarms.

Privileges	Description
System Configuration	To allow user to run the Windows SetMax configuration editor, save the current system environment as the default settings, or exit to Windows.
UserMacro Lock Unlock	To allow user to lock or unlock user macros.
ToolBar Buttons	
SalvoLayouts...	To allow user to add or access different salvolayouts.
Surrounding Camera	To allow user to view surrounding cameras.
Full Screen Mode	To allow user to view full screen mode.
Sync PlayBack Mode	To allow user to access the sync playback mode.
Remote Monitor Mode	To allow user to access the remote monitor mode.
Incident management Mode	To allow user to access the incident management mode.
Create Salvo	To allow user to create a salvo.
Application Launch Pad	To allow user to access the application launch pad.
Salvo Snapshot	To allow user to capture a salvo snapshot.
Instant Clip Export	to enable user to instantly export a clip.
Snapshot	To capture a snapshot.
Color Correction	Allow user to perform color correction.
Flip	Allow user to flip a video.
Mirror	Allow user to mirror view a video.
Preview	Allow user to preview a video.
Remove Text Overlay	Allow user to remove text overlay.
Analytics	
Add Analytics server	To add analytics server.
Update Analytics server	To update analytics server.
Delete Analytics server	To delete analytics server.
Launch HVA Configurator	To launch HVA configurator.
Launch HVA Live Monitor	To launch HVA Live Monitor.
Reports and Forsenics	To access the reports and forsenics.

Privileges	Description
Enable Analytics Option for Camera	To allow user to enable the analytics option for camera.

Note: To enable all the privileges select the Allow All check box and to deny all the privileges, select the Deny All check box.

7. Associate Partitions. See [Associating Partitions to the Roles](#) for more information.
8. Associate Workstations. [Associating Workstations to the Roles](#) for more information.
9. Click Save.

Associating Partitions to the Roles

You can associate partitions to roles. Associating partitions to a role enables a user to perform video surveillance tasks for all the video devices that are grouped in the partition.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partition to the role

1. Click the Configurator tab.
2. Expand the User Management branch in the navigation area, and then click Roles. The Roles screen appears in the display area.
3. Double-click the role you want to associate. The General Settings screen appears.
4. Click the Partitions tab. The screen displays the associated partitions, if any.

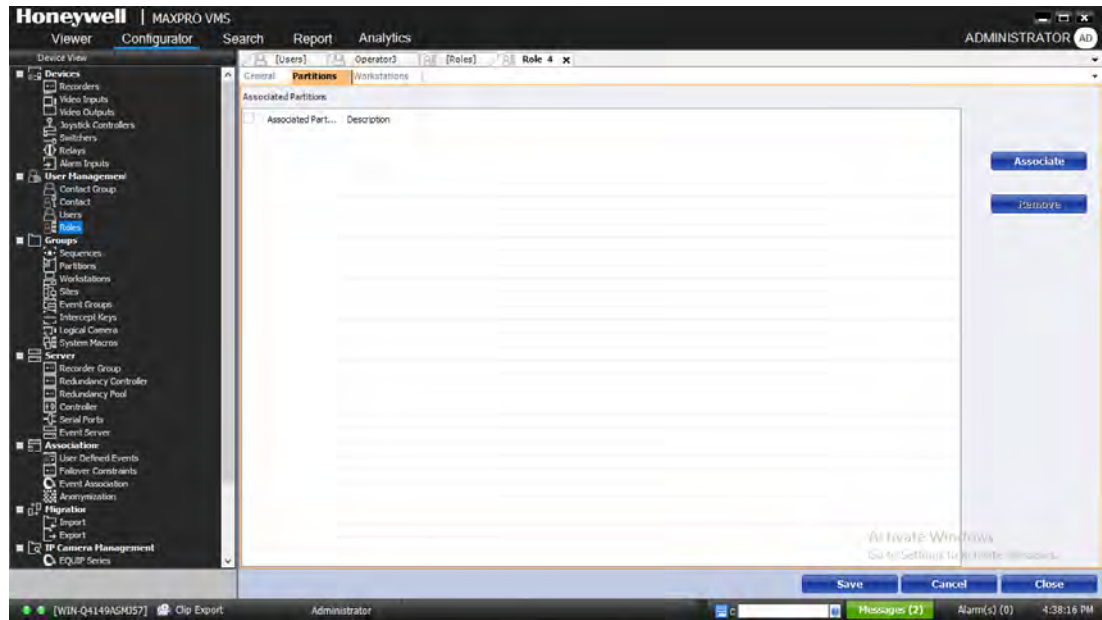


Figure 4-49 Roles Partitions

5. Click Associate. The Select Partitions page appears.
6. Select the check box corresponding to the partition name you want to associate.
7. Click OK.

To disassociate partitions from the role

- Select the check box corresponding to the partition name, and then click Remove.

Associating Workstations to the Roles

You can associate client workstations to roles to enable a user associated to the role to log on to MAXPRO VMS user interface and perform various actions.

Before you begin

- Add a Workstation. [Adding a Workstation](#) for more information.

To associate workstations to the role

1. Click the Configurator tab.
2. Expand the User Management branch in the navigation area, and then click Roles. The Roles screen appears in the display area.
3. Double-click the role you want to associate. The General Settings screen appears.
4. Click the Workstations tab. The screen displays the associated workstations, if any.

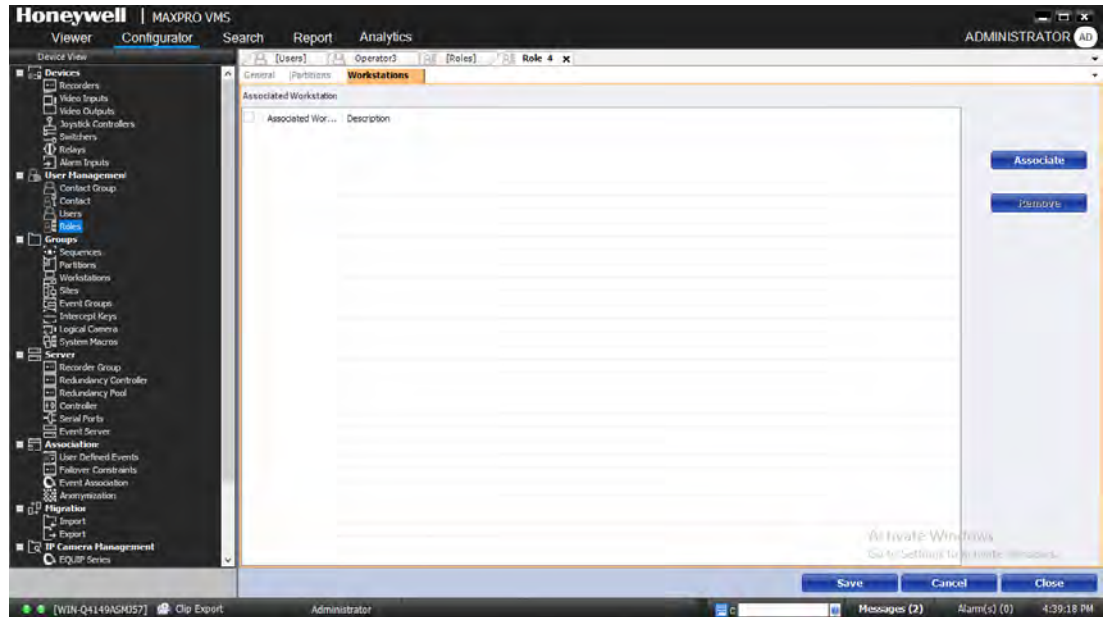


Figure 4-50 Roles Workstations

5. Click Associate. The Select User Workstation page appears.
6. Select the check box corresponding to the workstation name you want to associate.
7. Click OK.

To disassociate workstations from the role

- Select the check box corresponding to the workstation name, and then click Remove.

Updating a role

You can update the details of a role by changing the role name. In addition, you can also add or remove privileges to the role.

To update a role

1. Click the Configurator tab.
2. Expand the User Management branch in the navigation area, and then click Roles. The Roles screen appears in the display area.
3. Select the check box corresponding to the role you want to update.
4. Click Update. The general settings appear. You can modify the settings.

Deleting a role

You can delete a role from MAXPRO VMS. Before you delete a role, ensure that you remove all the associations made to it.

Before you begin

- Disassociate Partitions. See [Associating Partitions to the Roles](#) for more information.
- Disassociate Workstations. See [Associating Workstations to the Roles](#) for more information.

To delete a role

1. Click the Configurator tab.
2. Expand the User Management branch in the navigation area, and then click Roles. The Roles screen appears in the display area.
3. Select the check box corresponding to the role you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

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.

Note: 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 being captured from different cameras located across the sites.

To create a sequence

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Sequences. The Sequences screen appears in the display area.
3. Click Add. The Scan screen appears.
4. From the Sequence Type drop-down list, select the required sequence type. The available sequence types are listed in the table.
5. In the Description box, type a name for the sequence.
6. Follow steps 7 through 11 if you select Scan or Tour as scan type.

Sequence Type	Description
Scan	During a Scan sequence operation, camera selection entries are wrapped around when the end of the scan sequence is reached. This mode of operation continues until the scan sequence is halted.
Tour	During a Tour sequence, the scan sequence is stepped through only once.
Index	When Index is selected for this field, it indicates that the table is used to hold information for complex macro programming.

If you select index type:

- In the Sequence Type drop-down list, select Index.
 - Type the index value corresponding to the camera ID.
 - Click Save.
7. In the Dwell Time box, type the dwell time, in seconds, for the camera to display video before advancing to next camera.
 8. In the Select Cameras list, click . The Select from List page appears.
 9. Select the check box corresponding to the cameras that must be included in the sequence.
 10. Click OK to close the Select from List page. The cameras included in the sequence appear in the Select Cameras list.
 11. To include presets in the sequence, type the preset number in the Preset column next to a camera. The video from each camera in the list is displayed sequentially.

Note: If the value is zero in the preset column, the presets are not included in the sequence. By default, presets are zero for a fixed camera.

12. Click Save.

Playing a Sequence

To play a sequence



1. Click the Viewer tab.
2. Click the Sequences window.
3. Double-click the sequence you want to play or select the sequence, and then click Play Sequence. You can drag and drop the sequence on a panel in the salvo layout.

You can also play a sequence using the joystick controller (Ultrakey keyboard). See About [Joystick Controllers](#) for more information.

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  to move the camera one row up, or click  to move the camera one row down.
3. Click Save.

Removing Cameras from the Sequence

You can delete a camera from a sequence, when you do not want to view the live video from it as a part of the sequence. \

To remove cameras from a sequence

1. In the Select Cameras list, select the check box corresponding to the cameras you want to remove.
2. Click the  to remove the cameras from the sequence.
3. Click Save.

Removing Presets from the 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, delete the preset number next to the camera.
2. Click Save.

Locking a Sequence

You can lock an existing sequence to prevent the users from modifying it.

To lock a sequence

1. Select the Locked check box.
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.
2. Expand Groups in the navigation area, and then click Sequences. The Sequences screen appears in the display area.
3. Select the check box corresponding to the sequence you want to update.
4. Click Update. You can change the sequence of the cameras.

Deleting a Sequence

To delete a sequence

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Sequences. The Sequences screen appears in the display area.
3. Select the check box corresponding to the sequence.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Analytics

Analytics server enables smooth and effective daily surveillance operations. Analytics system is efficient in taking video inputs from live cameras, analyze the video content, and extract relevant information from the video. Automation of motion detection, triggering real-time alarms, and enabling fast search and retrieval of video are some of the distinct features of analytics.

Video Analytics takes video inputs from multiple live cameras, analyzes the video content in real-time, and extracts relevant information in the video. The system includes analytics servers, which analyze the content of the video, and various client GUI applications that can connect to the analytics servers to perform specific management or monitoring tasks. The applications can be launched directly from the server or from a separate client personal computer that can access the server through a TCP connection.

Honeywell Video Analytics (ActivEye) Reporting Tool

The Honeywell Video Analytics (ActivEye) Reporting Tool provides statistics report generation for any of the events detected in the system, including counting data as well as surveillance events. You can configure the reporting template and also set up scheduled e-mail reporting.

The Reporting Tool has three client applications:

- Honeywell Video Analytics (ActivEye) Reports Generator
- Honeywell Video Analytics (ActivEye) Reports Health Monitor
- Honeywell Video Analytics (ActivEye) Reports Scheduler

For more details, refer to the *Video Analytics V4 Reference Guide*.

To access the guide, choose Start>Programs>Honeywell Video Analytics>Documentation>Video Analytics V4 Reference Guide.pdf or locate the file in installation DVD.

Honeywell Video Analytics (ActivEye) Alarm Management

The Honeywell Video Analytics (ActivEye) Alarm Management component allows you to monitor the real-time alarms at a central station from multiple Video Analytics Servers. There are three components that enable the alarm management functionality:

- Honeywell Video Analytics (ActivEye) Alarm Watch Admin
- Honeywell Video Analytics (ActivEye) Alarm Watch Manager
- Honeywell Video Analytics (ActivEye) Alarm Watch Station

For more details, refer to the *Video Analytics V4 Reference Guide*.

To access the guide, choose Start>Programs>Honeywell Video Analytics>Documentation>Video Analytics V4 Reference Guide.pdf or locate the file in installation DVD.

Honeywell Video Analytics (ActivEye) Configuration Tool

Honeywell Video Analytics (ActivEye) configuration tool allows you to configure the rules in each camera view for your daily surveillance or operational needs.

For more details, refer to the *Video Analytics V4 Reference Guide*.

To access the guide, choose Start>Programs>Honeywell Video Analytics>Documentation>Video Analytics V4 Reference Guide.pdf or locate the file in installation DVD.

Honeywell Video Analytics (ActivEye) Forensics Tool

Honeywell Video Analytics (ActivEye) Forensics tool allows remote users to connect to the Video Analytics database on the server to conduct search and retrieval of past incidents.

For more details, refer to the Video Analytics V4 Reference Guide.

To access the guide, choose Start>Programs>Honeywell Video Analytics>Documentation>Video Analytics V4 Reference Guide.pdf or locate the file in installation DVD.

Honeywell Video Analytics (ActivEye) live Monitoring Station

Honeywell Video Analytics (ActivEye) Live Monitoring Station allows remote users to receive live video streams with analytics annotations as well as real-time events and alarms across multiple Analytics Servers.

For more details, refer to the Video Analytics V4 Reference Guide.

To access the guide, choose Start>Programs>Honeywell Video Analytics>Documentation>Video Analytics V4 Reference Guide.pdf or locate the file in installation DVD.

Honeywell Video Analytics (ActivEye) User Configuration

Honeywell Video Analytics (ActivEye) User Configuration allows managing user accounts. All the client applications require a valid user account to log on to the server and perform various tasks

For more details, refer to the Video Analytics V4 Reference Guide.

To access the guide, choose Start>Programs>Honeywell Video Analytics>Documentation>Video Analytics V4 Reference Guide.pdf or locate the file in installation DVD.

Adding an Analytics Server

To add an analytics server

1. Click the Configurator tab.
2. Expand the Servers branch in the navigation area, and then click Analytics. The Analytics Servers screen appears in the display area.

- Click Add. The general settings screen appears.

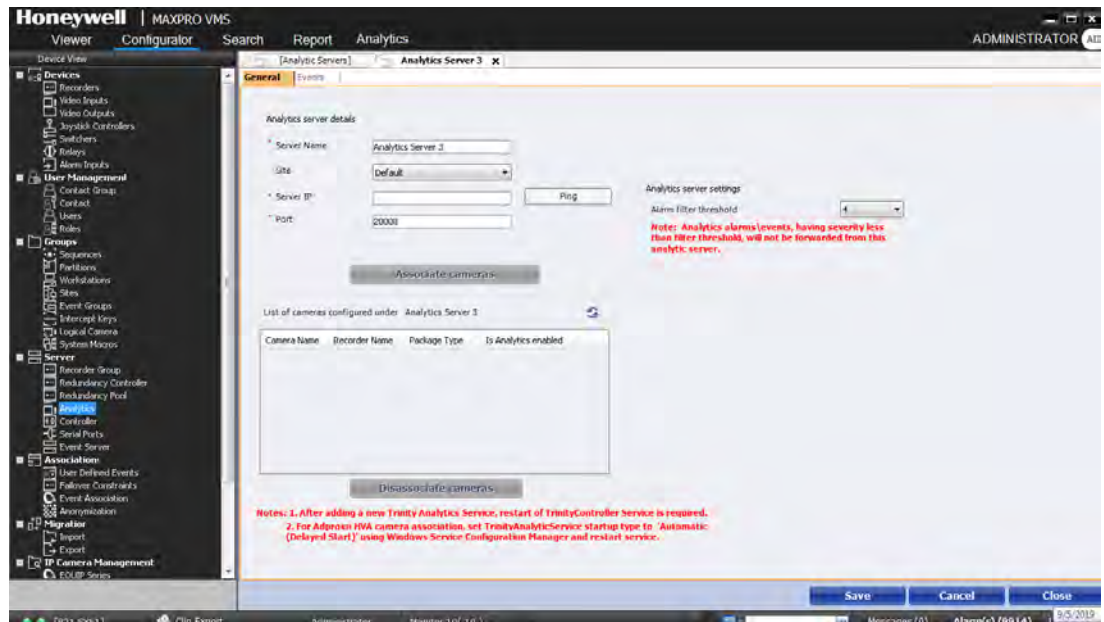


Figure 4-51 Analytics Server

- In the Server Name box, type a name for the server.
- From the Site drop-down list, select the required site.
- In the Server IP box, type the IP address of the server where the analytics is installed. Click Ping to verify the connection. The field appears in green if the IP address or the host name is valid.
- In the Port box, type the port number to connect the server.
- Click Save.

To associate cameras to analytics

- Click Associate Cameras. The Select camera list page appears.
- Select the cameras that have to be associated to analytics.
- From the Analytics package settings for the selected cameras drop-down list, select the required package, and then click Set analytics package type.

Note: The license information of each Honeywell Video Analytics (HVA) package is explained under the License Information section.

- Click Associate.
- Click Cancel to exit. The cameras are associated and displayed in the Analytical Server page.
- Associate Events and Events Attributes. See [Associating Events and Event Attributes to Analytics](#) for more information.

To disassociate cameras from analytics

1. In the List of Cameras configured under section, select the camera that you want to disassociate.
2. Click Disassociate Cameras.

Setting alarm filter threshold

1. From the Alarm filter threshold drop-down list, select a severity level for the alarm threshold.

Note: *This severity level is applicable only for Analytics alarms. If “alarm threshold value” is 4, then the events with severity level less than 4 are not stored in the Trinity database. However, you can view these events using the ActiveEye tool.*

Associating Events and Event Attributes to Analytics

You can associate one or more events to a analytics server. An alarm is triggered whenever any of the associated event occurs for the analytics server. For certain events, you can also associate event attributes. For example, for an Encoder Disabled event, you can associate attributes such as Encoder Name, Encoder ID and so on. For every attribute that you associate, you can set a value based on which the event is triggered. In the above example, you can associate the attribute Encoder Name to the event and set its value as Encoder A. When this event is associated to the video input, an alarm is raised when the event “Encoder Disabled” occurs for the Encoder Name “Encoder A”.

Attributes are available only for certain events. These events can be associated to a analytics multiple times. The event attributes are listed in the details of the alarm in Alarm window. To view the event attributes of an alarm, right-click the alarm, and then click Show Details.

To associate events to a analytics

1. Click the Events tab. The screen displays the associated events if any.
2. Click Associate. The Select Available Events page appears.
3. Select the check box corresponding to the event you want to associate.
4. Click OK.

To disassociate events from a analytics

- Select the check box corresponding to the event, and then click Remove.

To add Event Groups to events

1. Select the check box corresponding to the event you want to add the Event Group.
2. Double-click on the Event Group box. Select Event Groups page appears.
3. Click the check box corresponding to the Event Group you want to add.
4. Click OK.

To disassociate events from a analytics

- Select the check box corresponding to the event, and then click Remove.

Note: You need to add an event group before you associate it to an event. See [Adding an Event Group](#) for more information.

To disable an event

1. Select the check box corresponding to the event you want to disable.
2. Click the Disabled box. A drop-down list is enabled.
3. Select True.

To assign severity level

1. Select the check box corresponding to the event you want assign severity level.
2. Double-click on the Severity Level box and edit the severity level.

Note: Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

To enter remarks

1. Select the check box corresponding to the event you want to enter remarks.
2. Click the Remarks box and type the remarks.

To assign macros

1. Select the check box corresponding to the event you want to assign macros.
2. Click the Start Procedure box, and then type the required macro.
3. Click the End Procedure box, and then type the required macro.

Associating Event Attributes

Before you begin

- Associate events.

To associate event attributes

1. Select the check box corresponding to the event for which you want to associate event attributes. The Event attributes Settings appear in the lower pane.
2. Click Associate. The Select Available Event Attributes page appears.
3. Select the check box corresponding to the event attributes that you want to associate.
4. Click OK.

To disassociate event attributes from a analytics

- Select the check box corresponding to the event attribute, and then click Remove.

The following table describes the event name, event attributes, and their description

Event Name	Event Attributes	Attribute Description
Analytics server CPU is overloaded	CPU usage in percentage	CPU usage in percentage
Low disk space in analytics server	Free disk space in MB	Available free disk space in MB
Analytics server disk reaching minimum disk space	Free disk space in MB	Available free disk space in MB
Analytics server disk is healthy	Free disk space in MB	Available free disk space in MB

Partitions

A partition is a logical grouping of recorders, video inputs, switchers, and video outputs across various sites. Partitions are created for granting specific access rights to the users of MAXPRO VMS.

You can add a new partition by specifying a unique ID and a description. After adding a partition, you can add video devices to it.

You can also delete a partition when it is no longer needed. Before deleting a partition, disassociate the video devices from it and also unassign it from the user.

Default partition

A default partition is automatically created in MAXPRO VMS and all the newly added video devices are associated to it. Since, all the new devices are a part of the default partition, all users logging on to MAXPRO VMS can view them.

Partitions and Users

Partitions are associated to the users. They can view and manage the video devices that are grouped inside the associated partitions.

Partitions and Roles

Partitions are associated to roles. Roles are assigned to users. A user can view and manage the video devices that are grouped inside the associated partitions.

Partitions and video devices

Partitions are associated to devices like cameras, recorders, switchers and monitors. Users associated to a partition can view and manage all the devices grouped inside it.

Partitions and Monitors

Partitions are associated to monitors. Users associated to a partition can perform surveillance operations through monitors associated in that group.

Adding a Partition

You can add a partition by specifying a unique identification number and a description.

Note: By default, a global partition is added in MAXPRO VMS and all video devices are associated to it.

To add a partition

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Partitions. The Partitions screen appears in the display area.

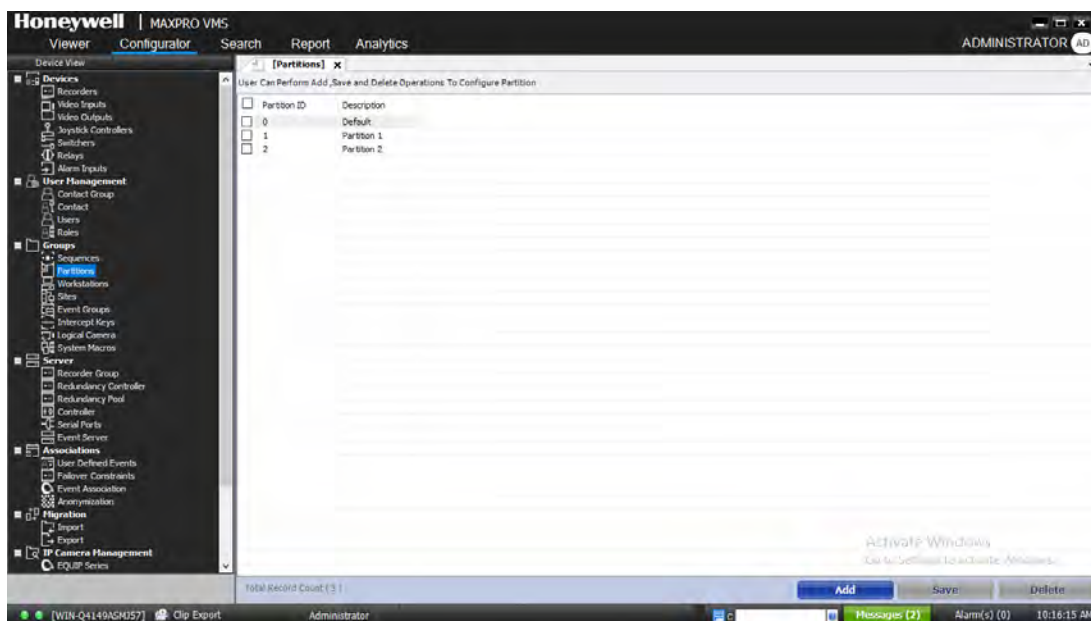


Figure 4-52 Partitions

3. Click Add. By default, the Partition ID and Description are displayed.

Note: You can change the default Partition ID and Description.

4. Click Save.

Deleting a Partition

You can delete a partition when you no longer need it. Before deleting a partition, ensure that you disassociate all video devices and unassign the user.

Before you begin

Disassociate all the devices, relays, users, and roles associated to the partition.

To delete a partition

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Partitions. The Partitions screen appears in the display area.
3. Select the check box corresponding to the partition you want to remove.
4. Click Delete. A confirmation message appears on the top of the display area.
5. Click Yes.

Workstations

A client workstation is a computer in which the MAXPRO VMS user interface is installed. A user can log on to MAXPRO VMS interface through workstations and perform various operations.

Workstations and Users

Users are directly associated to the workstation which is associated to the role. A user can be associated to other workstations which are not associated to a role.

See [Associating Workstations to the Users](#) for more information.

Workstations and Roles

Workstations are associated to Roles. Roles are assigned to users which enables them to log on to MAXPRO VMS interface and perform various actions.

See [Associating Workstations to the Roles](#) for more information.

Adding a Workstation

A user can log on to MAXPRO VMS user interface through client workstation. Workstation name is the computer name of the client computer.

To add a workstation

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Workstations. The Workstations screen appears in the display area.

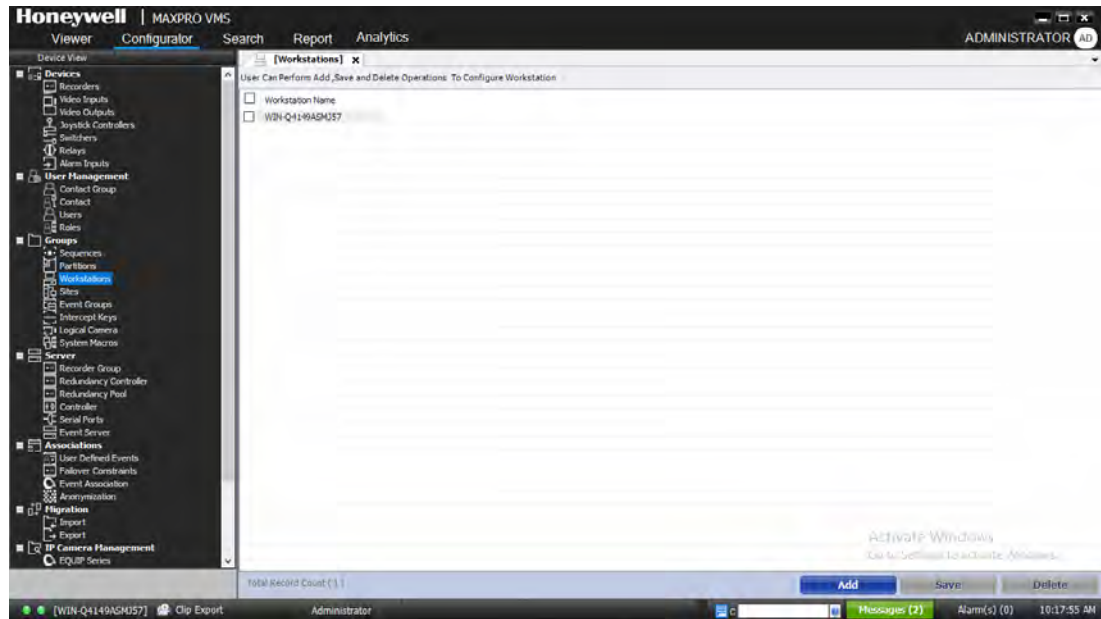


Figure 4-53 Workstations

3. Click Add. A new workstation gets added to the list.
4. Rename the workstation name if necessary.
5. Click Save.

Deleting a Workstation

You can delete a workstation. When you delete a workstation, all the associations made to the workstation are also removed.

To delete a workstation

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Workstations. The Workstations screen appears in the display area.
3. Select the check box corresponding to the workstation you want to remove.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Site

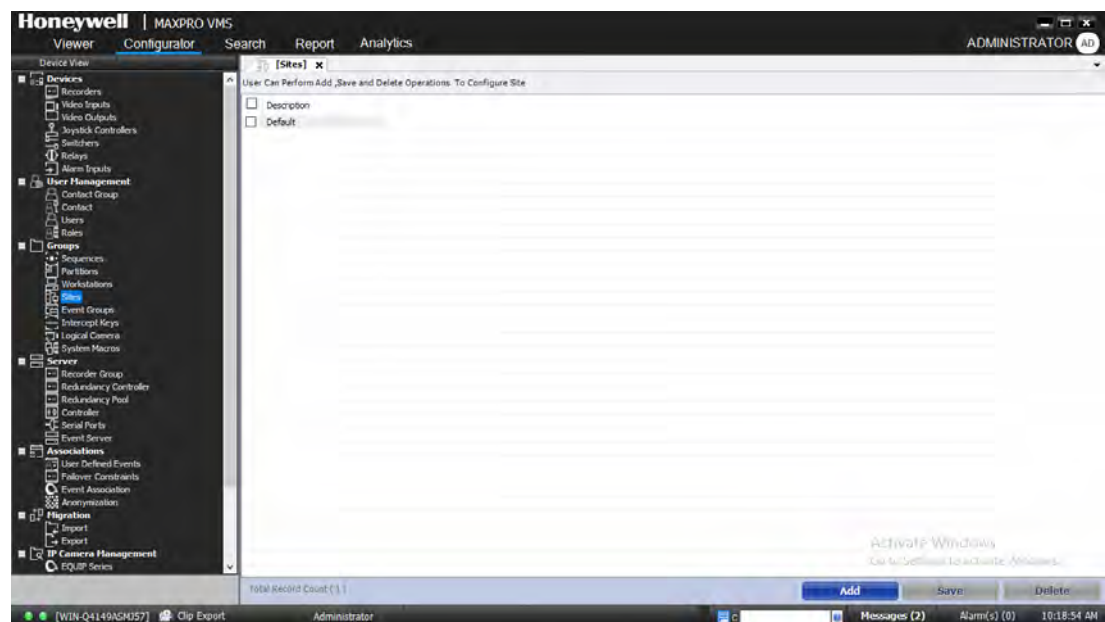
Site is a location where video input devices are situated. You can define more than one site in MAXPRO VMS. A default site is automatically created in MAXPRO VMS and all the video input devices can be associated to it.

Adding a Site

You can add a site to associate video inputs, recorders, switchers, video outputs, and workstations.

To add a site

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Sites. The Sites screen appears in the display area.



3. Click Add.
4. A new site gets added to the list. You can rename the site name if necessary.
5. Click Save.

Deleting a Site

Before you begin

- Disassociate all the associations to the site.

To delete a site

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Sites. The Sites screen appears in the display area.
3. Select the check box corresponding to the site you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Event Group

An event group is a grouping of events that occur on devices. The events that can occur vary based on the type of video devices.

For example, if a video connected to a recorder is lost, an event 'video loss' is generated. In MAXPRO VMS, an alarm is triggered whenever an event occurs.

Event groups are created for providing privileges to the users for viewing or acknowledging the events that occur on the video devices. By default, 99 Event Groups are added in MAXPRO VMS. Events that occur on the devices are grouped under different Event Groups. By default, all the events that can occur on devices are associated to Event Group 1.

Event Groups and Users

Event groups are associated to users. When any events in the event group occur, only the associated users can acknowledge it. See [Associating Event Groups to Users](#) for more information.

Event Groups and Monitors

Event groups are associated to monitors. When any event in the event group occurs, the event details are displayed in the associated monitors for viewing. See [Associating Video Outputs to Event Groups](#) for more information.

Adding an Event Group

You can add an event group to provide privileges for a user to acknowledge the events that occur on video devices.

To add an event group

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Event Groups. The Event Groups screen appears in the display area.
3. Click Add.
4. In the Event Group ID and Description column, a default reference number and a description for the event group appear by default.

5. Click Save.

Deleting an Event Group

You can delete an event group from MAXPRO VMS. Before deleting an event group, ensure that you disassociate the users and monitors from it.

Before you begin

- Disassociate Video Outputs. [Associating Events and Event Attributes to a Video Input](#) for more information.
- Disassociate Users. See [Associating Event Groups to Users](#) for more information.

To delete an event group

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Event Groups. The Event Groups screen appears in the display area.
3. Select the check box corresponding to the event group you want to remove.
4. Click Delete. A confirmation message appears on the top of the display area.
5. Click Yes.

Intercept Keys

Frequently used or repetitive sequence of keystrokes can be automated using intercept keys.

Intercept Keys and Joystick Controllers

Joystick controllers (Ultrakey keyboards) are associated to intercept keys. You can program the keys in the Ultrakey keyboard to perform an action by associating intercept keys to them. For example, a key can be programmed to select a panel in the salvo layout.

Adding Intercept Key

To add an intercept key

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Intercept Keys. The Intercept Keys screen appears in the display area.

3. Click Add. The General Settings screen for Intercept Keys displays.

Figure 4-54 Intercept Keys- General Settings

4. In the Intercept Key ID box, next available number is assigned by default.
5. In the Key Code box, type the key code of the key that is to be intercepted.
6. In the Intercept Key Description box, type a description for the intercept key for reference, if required.

Note: A default sequential Intercept Key name appears in the Intercept Key Description box.

7. In the Key Replacement Macro box, type the desired key replacement macro.

Note: When the specified key press on the selected keyboards is detected, the Key Replacement Macro is executed.

8. In the Key Release Macro box, type the desired key release macro.

Note: When the specified key on the selected keyboards is detected, the Key Release Macro is executed.

9. Associate Joystick Controller. See [Associating Joystick Controllers to Intercept Keys](#) for more information.
10. Click Save.

To restore default intercept keys

- Click Restore.

Associating Joystick Controllers to Intercept Keys

To associate joystick controller to intercept keys

1. Click the Joystick Controller tab. The Joystick Controller screen appears.
2. Click Associate. The Select Joystick Controllers page appears.
3. Select the check box corresponding to the joystick name you want to associate.
4. Click OK.

Note: By default, 99 joystick controllers are available in MAXPRO VMS.

To disassociate joystick controller from intercept keys

- Select the check box corresponding to the joystick name, and then click Remove.

Updating Intercept Keys

You can update intercept keys to change the key press number and change the description.

To update intercept keys

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Intercept Keys. The Intercept Keys screen appears in the display area.
3. Select the check box corresponding to the intercept key you want to update.
4. Click Update. The general settings for the intercept key appear. You can modify the settings according to your needs.

Deleting Intercept Keys

To delete intercept keys

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Intercept Keys. The Intercept Keys screen appears in the display area.
3. Select the check box corresponding to the intercept key you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Logical Camera

Logical camera selection allows cameras to be grouped together so that selection of a particular camera is made more easy for the user. Instead of selecting the camera by its number, the user can select the group the camera belongs to, followed by a number within that group. For example, Camera 1234 can instead be

selected as 'Level 1 Cameras', '5', with the name of the group (in this case Level 1 Cameras) being selected by a single button press. This speeds up and simplifies the selection of video inputs.

You can add a logical camera and associate it to the Joystick Controller.

Before you begin

- Add Camera. See [Adding a Camera](#) for more information.
- Configure Joystick Controller. [Configuring joystick controller](#) for more information.

Adding a Logical Camera

To add a logical camera

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Logical Camera. The Logical Camera screen appears in the display area.
3. Click Add. The Group screen for Logical Camera displays.

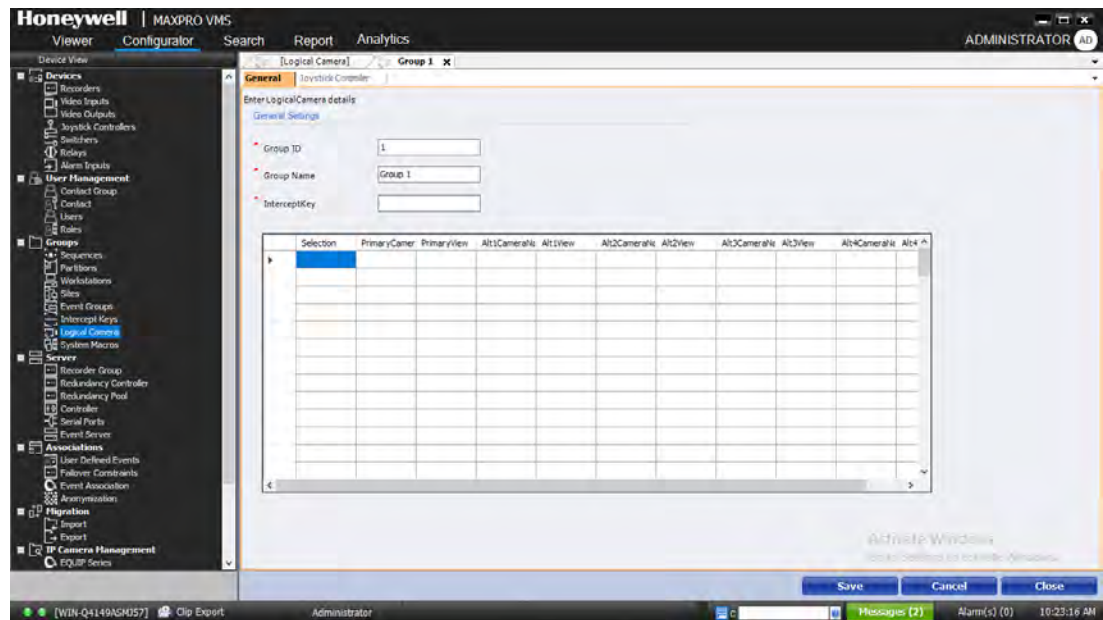


Figure 4-55 Logical Camera- General Settings

4. In the Group ID box, type the unique ID.
5. In the Group Name box, type a name for the logical group.
6. In the Intercept Key box, type a kicked number to select the group.

Note: Typing a number in the Intercept Key field automatically updates the Intercept Keyboard Keys table.

7. Specify the following details in the table.

Features	Description
Selection Number	Type a unique number within each group. It defines the number entered by the operator to select the Primary Camera in the group. There can be up to 99 different selection numbers per group. Valid values are 1 – 9999.
Primary Camera	Specify camera number that is selected when the operator selects a Group and a selection number within that group. Valid values are 1 – 9999, and must correspond to a camera number defined in the Video Inputs table.
Primary Camera View	The primary camera can also be a PTZ camera with view recall capability. In this case an actual View number can be specified. Therefore, selecting the group and selection number within that group not only displays the primary camera but also automatically moves it to the designated View preset position. The valid camera views range is 1 – 99, 0 is the default value which indicates no camera view is to be selected. As the view number '0' is used for indicating that NO VIEW is specified, view '0' can NOT be recalled by this field.
Alternate Camera 1	This field defines the first alternate camera to be selected when the 'ALT' key is pressed. This camera is also selected by pressing the ? key on the keyboard after the primary camera has been selected, or the ? key after the Alternate Camera 2 has been selected. The range of valid camera numbers is 1 – 9999. The alternate camera 1 would have to be defined elsewhere in the video input table. A value of 0 is the default value and indicates no alternate camera is defined.
Alternate Camera View	When Alternate Camera 1 is selected, it can automatically move to the designated View preset position. The valid camera views range is 1 – 99, Note: 0 is the default value which indicates no camera view is to be selected. As the view number '0' is used for indicating that NO VIEW is specified, view '0' can NOT be recalled by this field.
Alternate Camera 2	Define the second alternate camera to be selected when the 'ALT' key is pressed again after selecting alternate camera 1. The range of valid camera numbers is 1 – 9999. The alternate camera 2 must be defined elsewhere in the video input table. A value of 0 is the default value and indicates no alternate camera is defined.
Alternate View	When Alternate Camera 2 is selected, it can automatically move to the designated View preset position. The valid camera views range is 1 – 99, Note: 0 is the default value which indicates no camera view is to be selected. As the view number '0' is used for indicating that NO VIEW is specified, view '0' can NOT be recalled by this field.
Alternate Camera 3	Define the third alternate camera to be selected when the 'ALT' key is pressed again after selecting alternate camera 2. The range of valid camera numbers is 1 – 9999. The alternate camera 3 has to be defined elsewhere in the video input table. A value of 0 is the default value and indicates no alternate camera is defined.

Features	Description
Alternate View	When Alternate Camera 3 is selected, it can automatically move to the designated View preset position. The valid camera views range is 1 – 99, Note: 0 is the default value which indicates no camera view is to be selected. As the view number '0' is used for indicating that NO VIEW is specified, view '0' cannot be recalled by this field.
Alternate Camera 4	This field defines the fourth alternate camera to be selected when the 'ALT' key is pressed again after selecting alternate camera 3. The range of valid camera numbers is 1 – 9999. The alternate camera 4 would have to be defined elsewhere in the video input table. A value of 0 is the default value and indicates no alternate camera is defined.
Alternate View	When Alternate Camera 4 is selected it can automatically move to the designated VIEW preset position. The valid camera views range is 1 – 99, Note: 0 is the default value which indicates no camera view is to be selected. As the view number '0' is used for indicating that NO VIEW is specified, view '0' cannot be recalled by this field.

Note: Pressing the ALT key continuously on the keyboard cycles around the Primary camera and Alternate cameras defined in the group. Using the upper arrow and lower arrow keys selects the next or previous camera in the group until the last defined camera has been selected. Then an “End of Sequence” message is displayed on the user’s monitor.

8. Associate Joystick Controller. See [Associating Joystick Controllers to Logical Camera](#) for more information.
9. Click Save.

Associating Joystick Controllers to Logical Camera

To associate joystick controller to logical camera

1. Click the Joystick Controller tab. The Joystick Controller screen appears.
2. Click Associate. The Select Joystick Controllers page appears.
3. Select the check box corresponding to the joystick name you want to associate.
4. Click OK.

Note: By default, 99 joystick controllers are available in MAXPRO VMS.

To disassociate joystick controller from logical camera

- Select the check box corresponding to the joystick name, and then click Remove.

Deleting A Logical Camera

To delete logical camera

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Logical Camera. The Group screen appears in the display area.
3. Select the check box corresponding to the logical camera that you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes.

Updating Logical Cameras

You can update logical cameras to change the group name or the alternative camera.

To update logical cameras

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click Logical Camera. The Group screen appears in the display area.
3. Select the check box corresponding to the logical camera you want to update.
4. Click Update. The general settings for the logical camera appear. You can modify the settings according to your needs.

System Macros

A macro is a rule or pattern that specifies how a certain input sequence (often a sequence of characters) is mapped to an output sequence or action.

Adding a System Macro

You can add a macro to enter a single character or a word to perform a series of actions.

To add a system macro

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click System Macros. The System Macros screen appears in the display area.

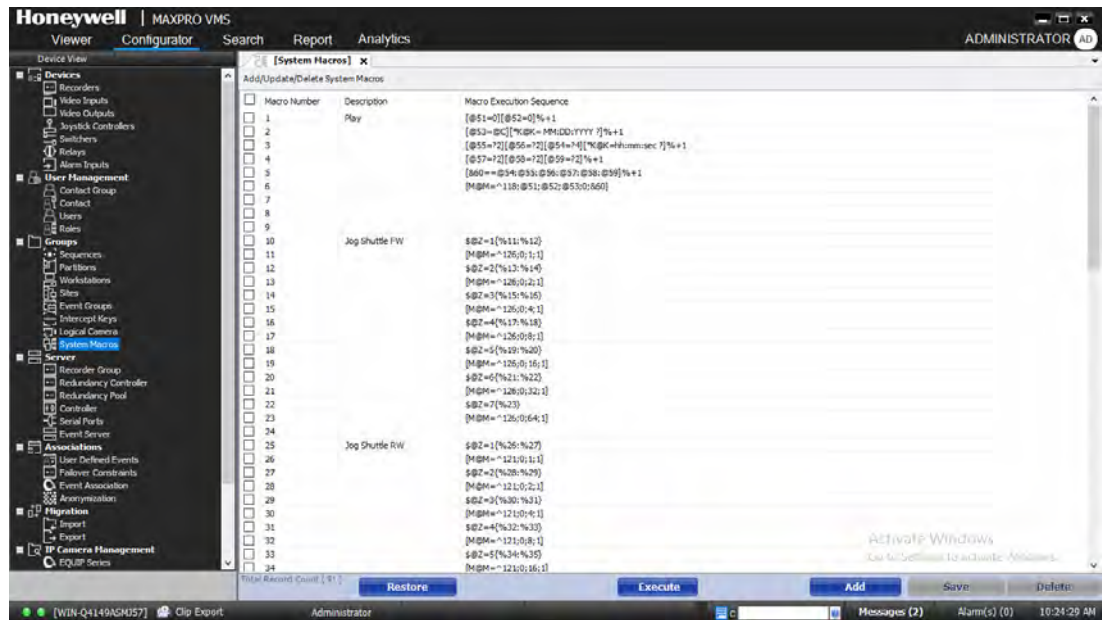


Figure 4-56 System Macros

3. Click Add. A System Macro is added.
4. In the Description column, type a description for the system macro for reference.
5. In the Macro Execution Sequence column, type the key press sequence or special command to perform the required function.

Executing a System Macro

MAXPRO VMS provides a feature to execute a system macro as and when it is created.

To execute a system macro

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click System Macros. The System Macros screen appears in the display area.
3. Select the check box corresponding to the system macros you want to execute. The desired macro is executed.

Note: Click Restore, to restore all the system macros to their factory default settings. The following message appears "All macros will be reset to factory default. All your modifications will be removed. Do you want to Proceed?". Click Yes or No as applicable.

Deleting a System Macro

To delete a system macro

1. Click the Configurator tab.
2. Expand Groups in the navigation area, and then click System Macros. The System Macros screen appears in the display area.
3. Select the check box corresponding to the system macros you want to delete.
4. Click Delete. A confirmation message appears on top of the display area.
5. Click Yes to remove the system macro.

Recorder Groups

Recorder group feature distributes the load on a controller. It allows you to create different groups and associate recorders to it. Associating recorders to the groups enables, the load is distributed among the recorder controllers. You can add, update and delete recorders in a specific group. Based on the load you can create maximum number of groups and associate recorder to each group. By default five groups are displayed.

Associating recorder to Recorder Groups

To associate recorder to recorder groups

1. Click the Configurator tab.
2. Expand the Servers branch in the navigation area, and then click Recorder Group. The Recorder Group screen appears in the display area with default recorder groups.

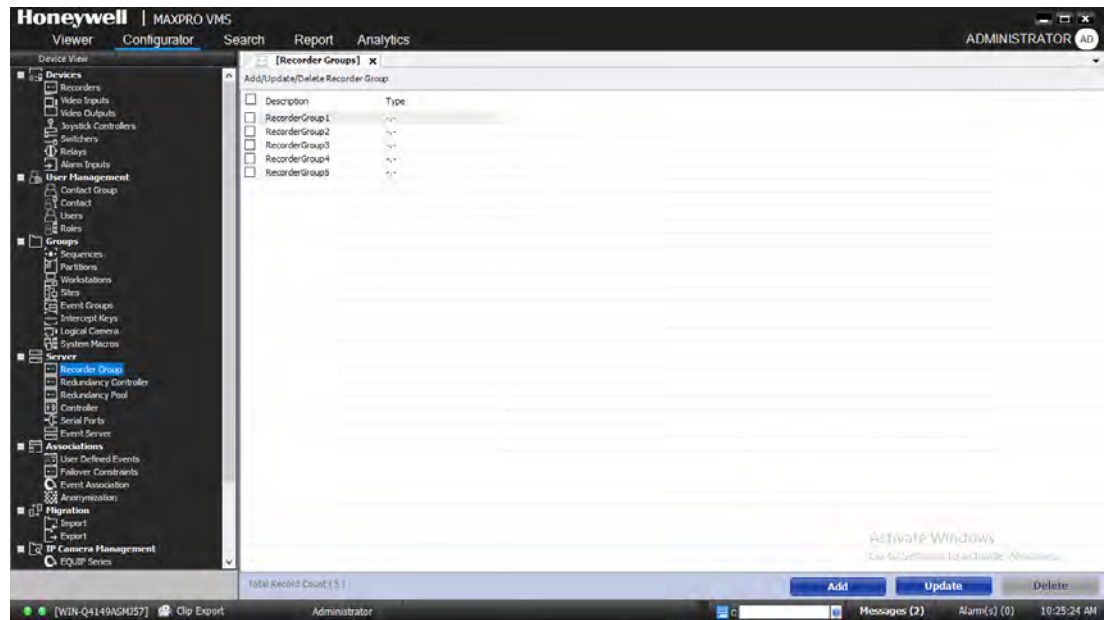


Figure 4-57 Recorder Group Screen

3. Click Add. The General settings screen for Recorder Group displays.

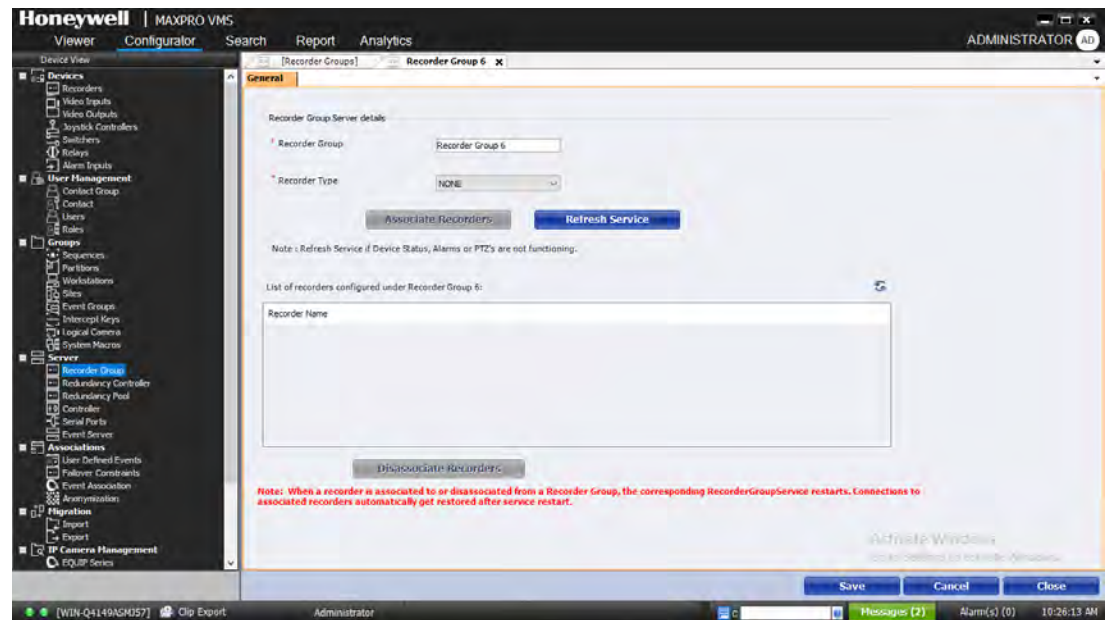


Figure 4-58 Recorder Group- General Settings

4. In the Recorder Group box, type a name for the recorder group.
5. In the Recorder Type drop-down list, select the recorder that you want to associate.

- Click Save. The Associate Recorders and Disassociate Recorders buttons are activated.
- Click Associate Recorders. The Select from list to Associate Recorder Group Server page appears.

Figure 4-59 Select from list - Associate

Disassociating Recorders from the Recorder Groups

1. In the List of Recorders configured under Recorder Group, click Disassociate Recorder. The Select from list to dissociate Recorder page appears.



Figure 4-60 Select from list - Disassociate

2. Select the Recorder from the list and then click Disassociate. The selected recorders are successfully disassociated from the Recorder Group message is displayed.

Updating Recorder Group

To update a recorder group

1. In the Recorder Groups screen, select the required Recorder Group check boxes.
2. Click Update. The General settings screen for Recorder Group displays.
Or
Double-click the required recorder group from the list. The General settings screen for specific Recorder Group displays.

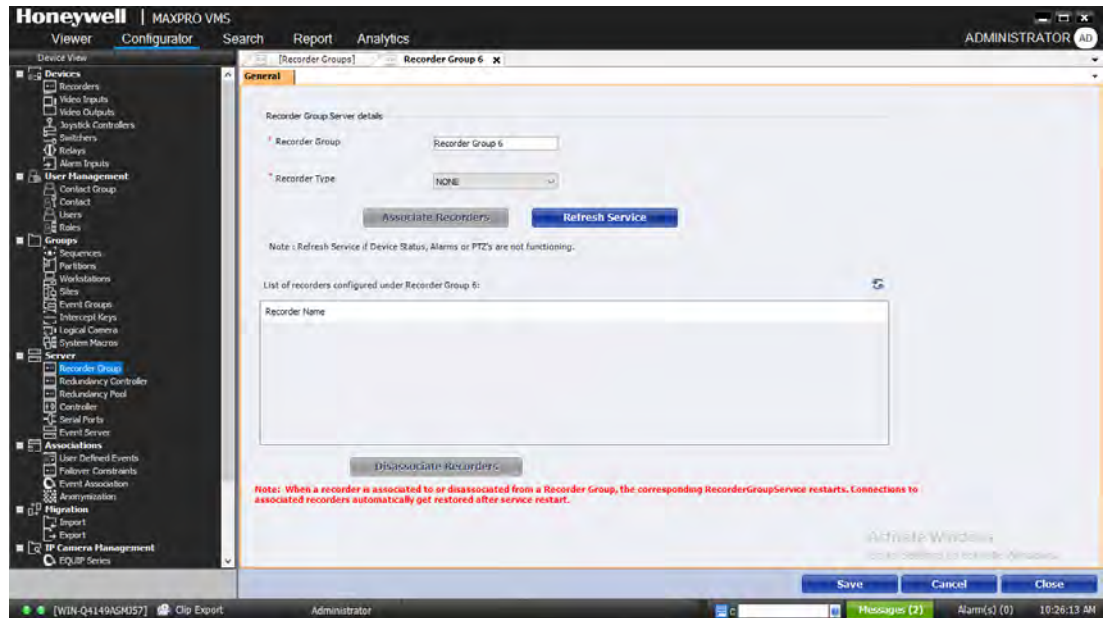


Figure 4-61 Update Recorder Group

3. Repeat the steps 7 and step 8 of [Associating recorder to Recorder Groups](#) to associate recorder.
4. Repeat the steps of [Disassociating Recorders from the Recorder Groups](#) to disassociate recorders.
5. Click Close.

Deleting Recorder Group

To delete the recorder groups you need to first disassociate the recorders under that group. See [Disassociating Recorders from the Recorder Groups](#).

Note: Deleting recorder group deletes the recorder service but the load is carried over to the actual controller service.

To delete a recorder group

1. In the Recorder Groups screen, select the required Recorder Group check box.
2. Click Delete. A confirmation message Do you really want to delete selected recorder group is displayed.
3. Click Yes to delete.

Redundancy Controller

Redundancy controller feature controls the redundancy options on a specific recorder. You can associate/disassociate, update and delete specific recorders that can be used under redundancy controller. Currently MAXPRO NVR Recorder supports Redundancy feature.

Configuring Redundancy Controller

To configure redundancy controller

1. Click the Configurator tab.
2. Expand the Servers branch in the navigation area, and then click Redundancy Controller. The Redundancy Controller screen appears in the display area.

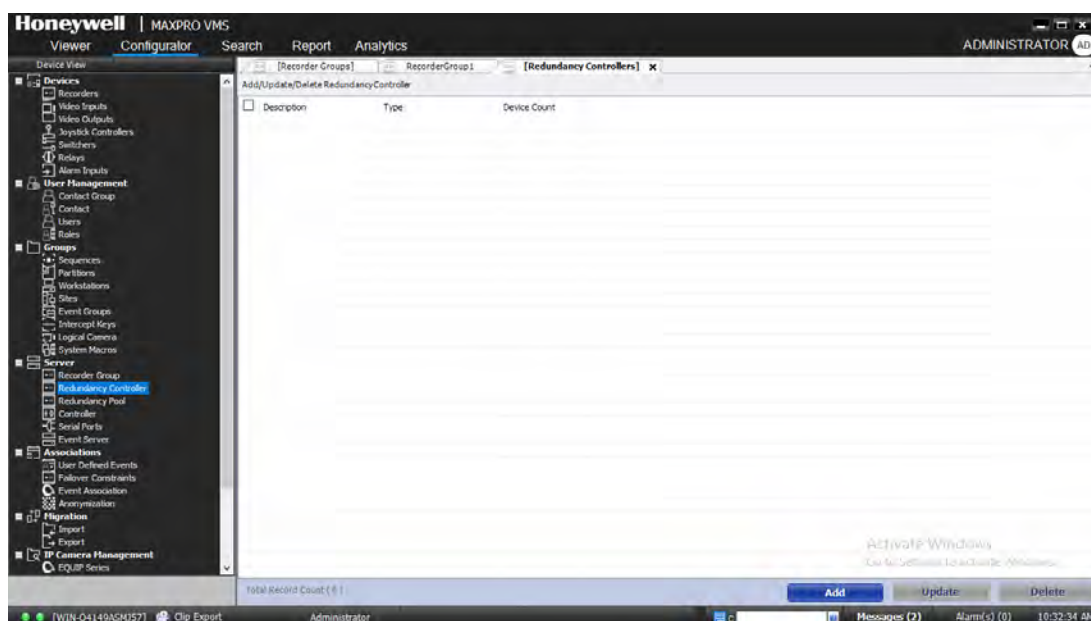


Figure 4-62 Redundancy Controller screen

3. Click Add. The General settings screen for Redundancy Controller displays.

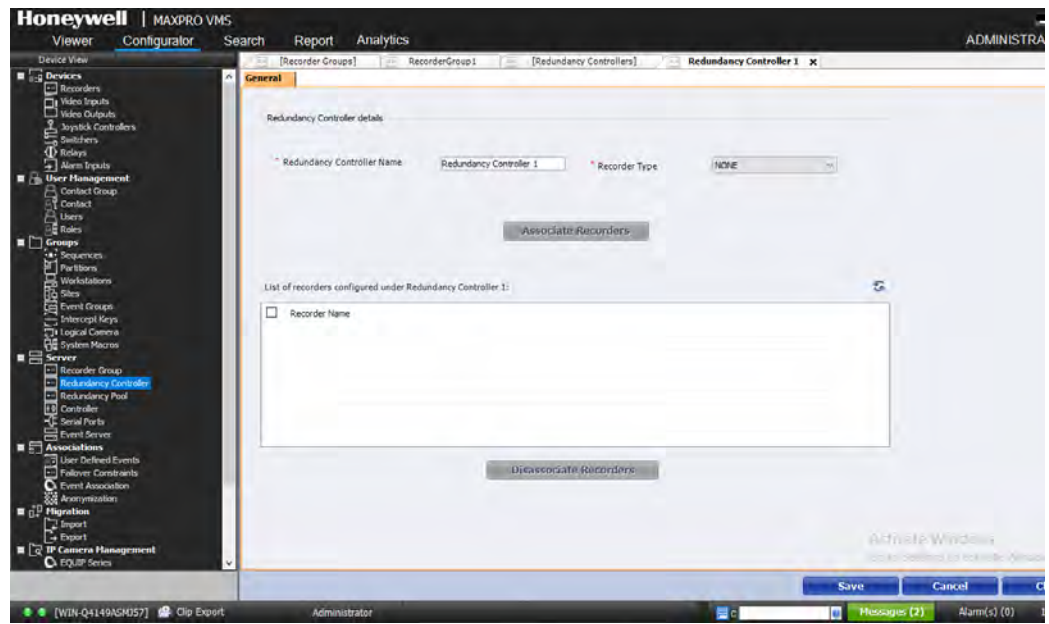


Figure 4-63 Redundancy Controller-General Settings

4. In the Redundancy Controller Name box, type a name for the controller.
5. In the Recorder Type drop-down list, select the recorder that you want to associate. Currently MAXPRO NVR recorder supports this feature.
6. Click Save. The Associate Recorders button is activated.
7. Click the Associate Recorders button. The Select from list to Associate Redundancy Controller page appears.

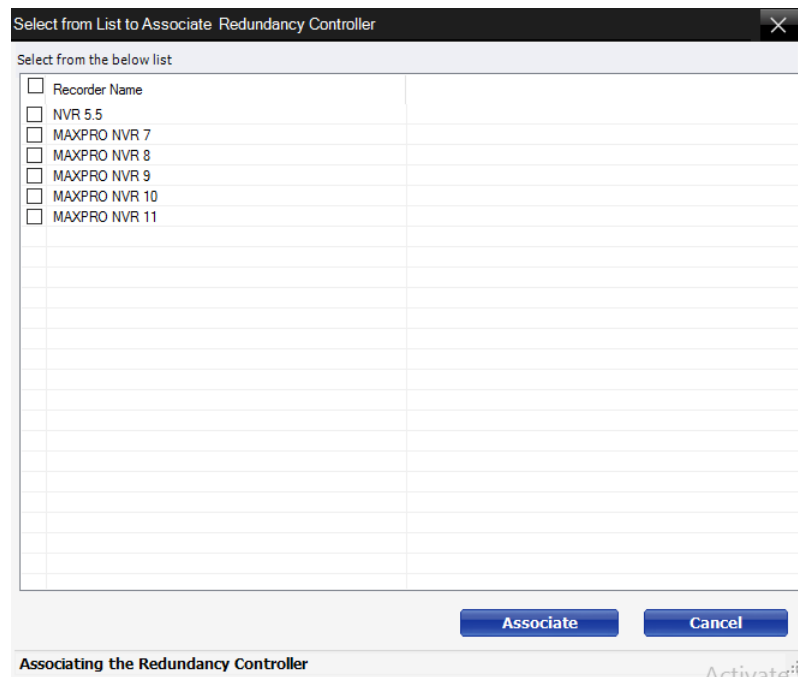


Figure 4-64 Select from list - Associate

8. Select the required Recorder from the list and then click Associate Recorders. The list of recorders associated for a controller is displayed under List of Recorders configured under Redundancy Controller as shown below.

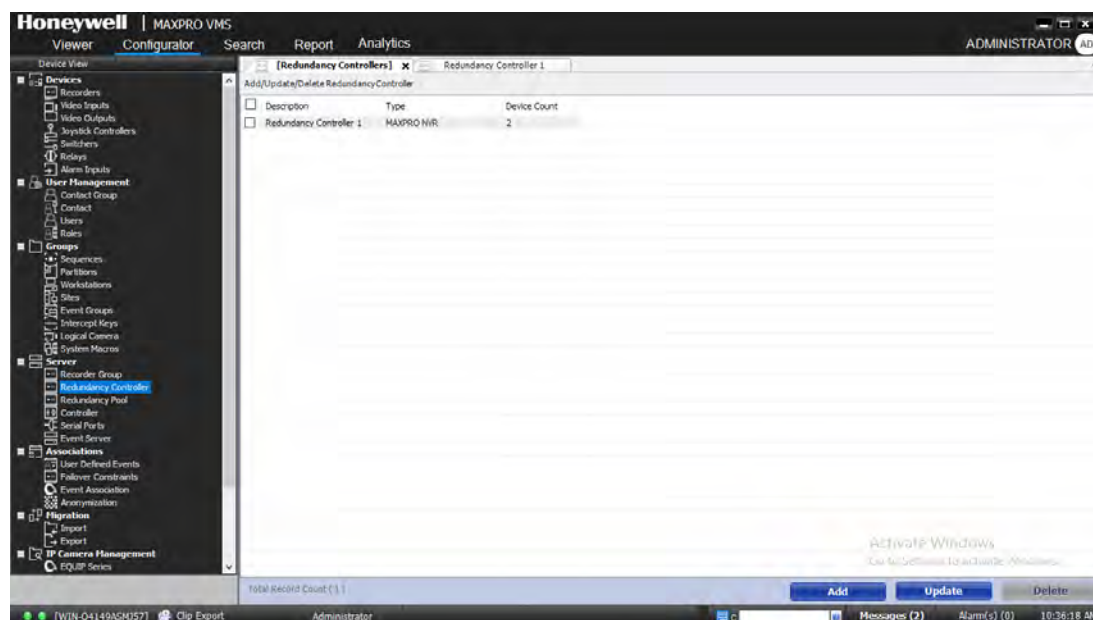


Figure 4-65 list of Redundancy Controllers

Disassociating Recorders from the Redundancy Controller

To dissociate recorders from the Redundancy Controller

1. Navigate to General settings screen of the required Redundancy Controller.
2. In the List of Recorders configured under Redundancy Controller table, select the Recorder from the list and then click Disassociate Recorders. The select recorder is removed from the list.

Updating Redundancy Controller

To update a redundancy controller

1. In the Redundancy Controllers screen, select the required Redundancy Controller check boxes from the list.
2. Click Update. The General settings screen for Redundancy Controller displays.
Or
Double-click the required redundancy controller from the list. The General settings screen for specific Redundancy Controller displays.

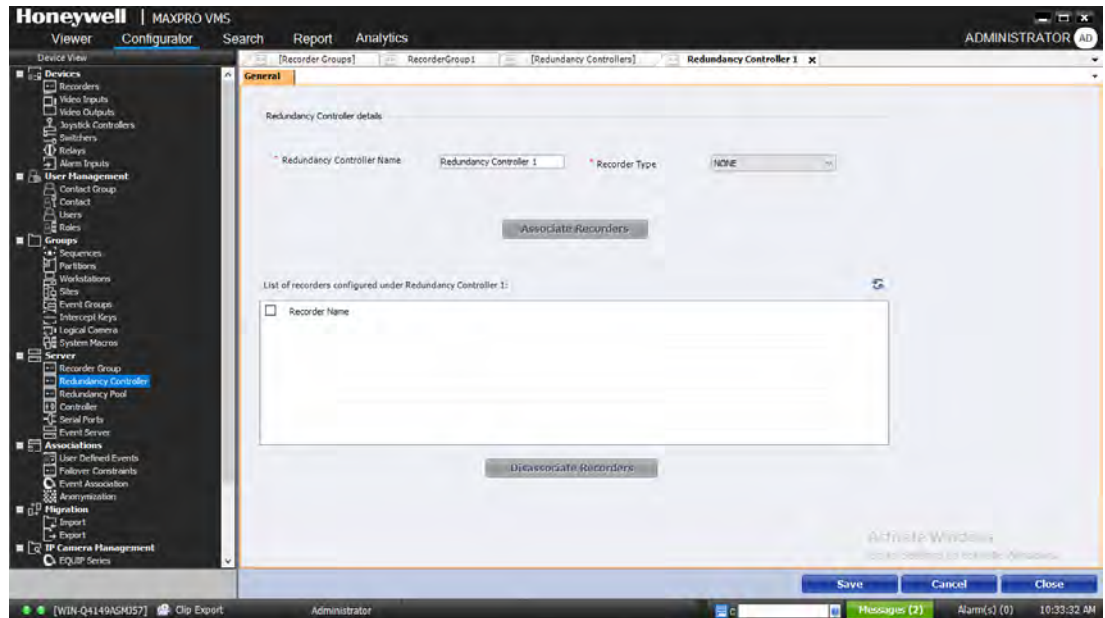


Figure 4-66 Update Redundancy Controller

3. Repeat the steps 7 and step 8 of [Configuring Redundancy Controller](#) to associate recorder.
4. Repeat the steps of [Disassociating Recorders from the Redundancy Controller](#) to disassociate recorders.
5. Click Close.

Deleting Redundancy Controller

To delete the Redundancy Controller you need to first disassociate the recorders under that controller. See [Disassociating Recorders from the Redundancy Controller](#).

To delete a Redundancy Controller

1. In the Redundancy Controllers screen, select the required Redundancy Controller check box.
2. Click Delete. A confirmation message Do you really want to delete selected Redundancy Controller is displayed.
3. Click Yes to delete.

Redundancy Pool

Redundancy Pool feature allows you to define the primary and redundant NVR recorders to manage the load in case of failover. It helps you to logically group the set of primary and failover recorder. You need to associate the required primary

and redundant recorders to configure the redundancy pool. This feature also allows you to update and delete required recorders. Currently MAXPRO NVR Recorder supports this feature.

Configuring Redundancy Pool

To configure redundancy pool

1. Click the Configurator tab.
2. Expand the Servers branch in the navigation area, and then click Redundancy Pool. The Redundancy Pool screen appears in the display area.

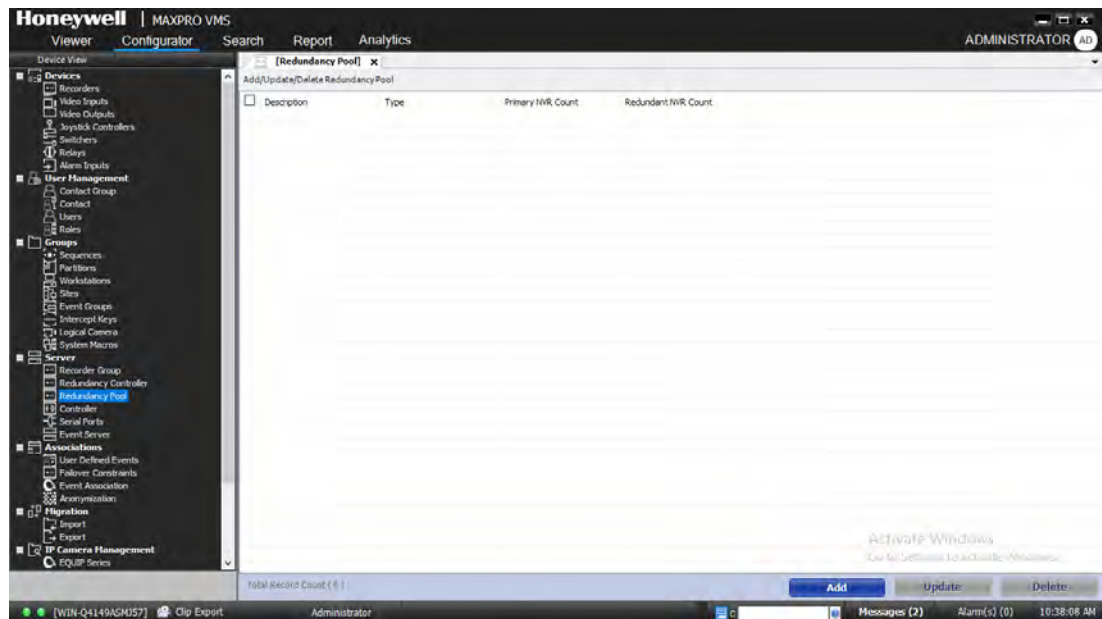


Figure 4-67 Redundancy Pool screen

3. Click Add. The General settings screen for Redundancy Pool displays.

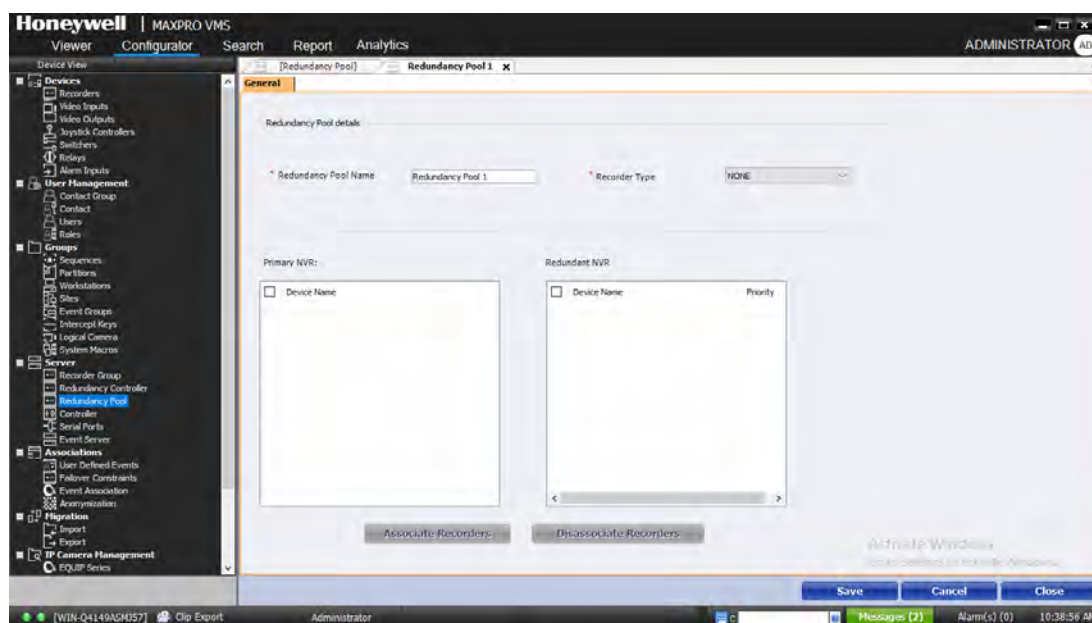


Figure 4-68 Redundancy Pool-General Settings

4. In the Redundancy Pool Name box, type a name for the pool.
5. In the Recorder Type drop-down list, select the recorder that you want to associate. Currently MAXPRO NVR recorder supports this feature.
6. Click Save. The Associate Recorders button is activated.
7. Click the Associate Recorders button. The Select from list to Associate Redundancy Pool page appears.

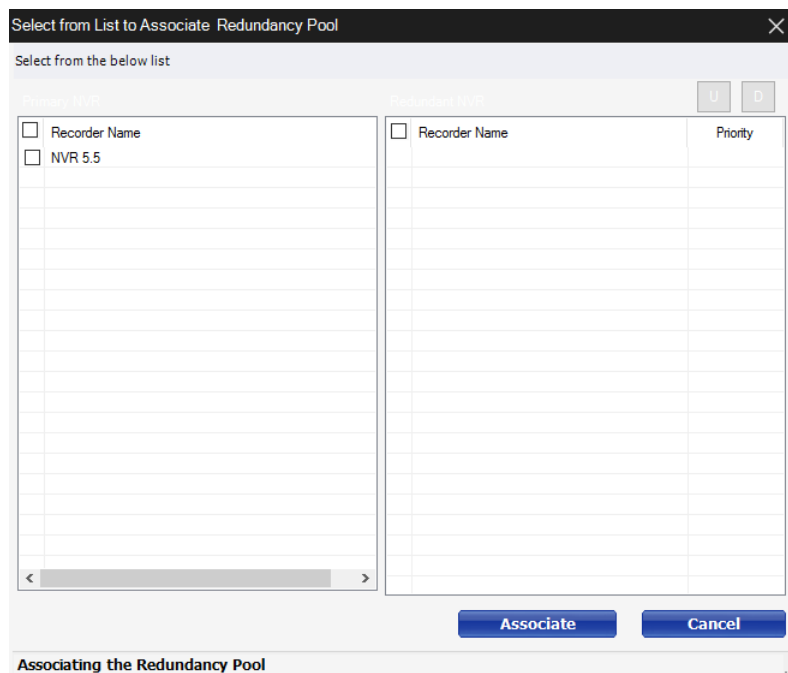


Figure 4-69 Select from list - Associate

8. In the Primary NVR pane, select the required recorder check box from the list to define as primary NVR recorders.
9. In the Redundant NVR pane, select the required recorder check box from the list to define as redundant NVR recorders.
10. Click Associate. The list of recorders associated under a pool is displayed under corresponding primary and redundant NVR panes.

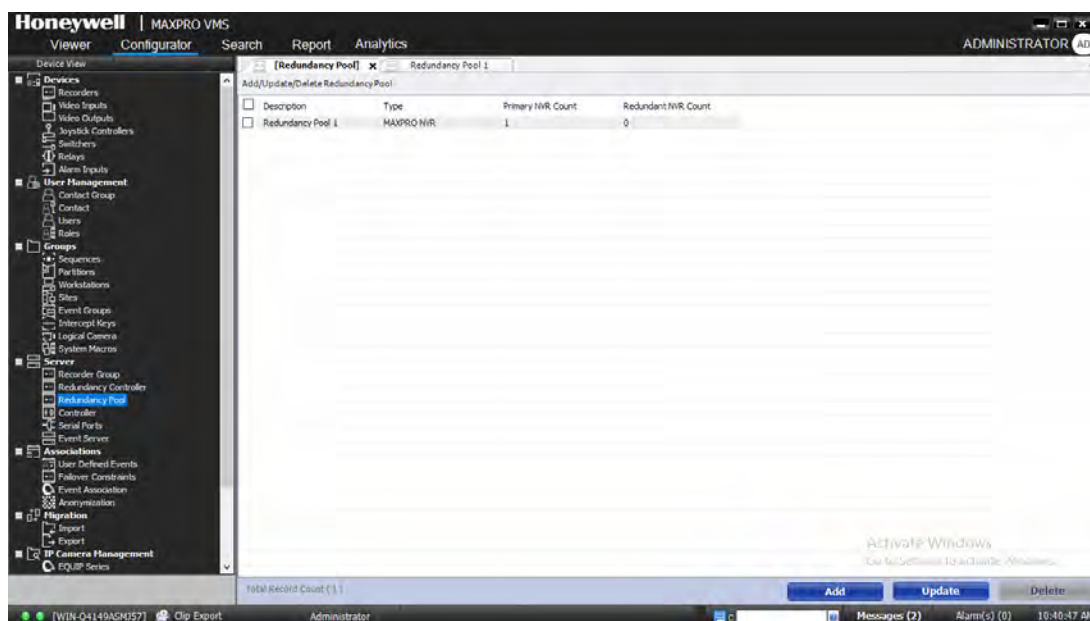


Figure 4-70 List of Redundancy Pools

Disassociating Recorders from the Redundancy Pool

To dissociate recorders from the Redundancy Pool

1. Navigate to General settings screen of the required Redundancy Pool.
2. Select the required recorders from the Primary and Redundant panes and then click Disassociate Recorders. The selected recorders are removed from the list.

Updating Redundancy Pool

To update a redundancy Pool

1. In the Redundancy Pool screen, select the required Redundancy Pool check boxes from the list.
2. Click Update. The General settings screen for Redundancy Controller displays.
Or

Double-click the require redundancy pool from the list. The General settings screen for specific redundancy pool displays.

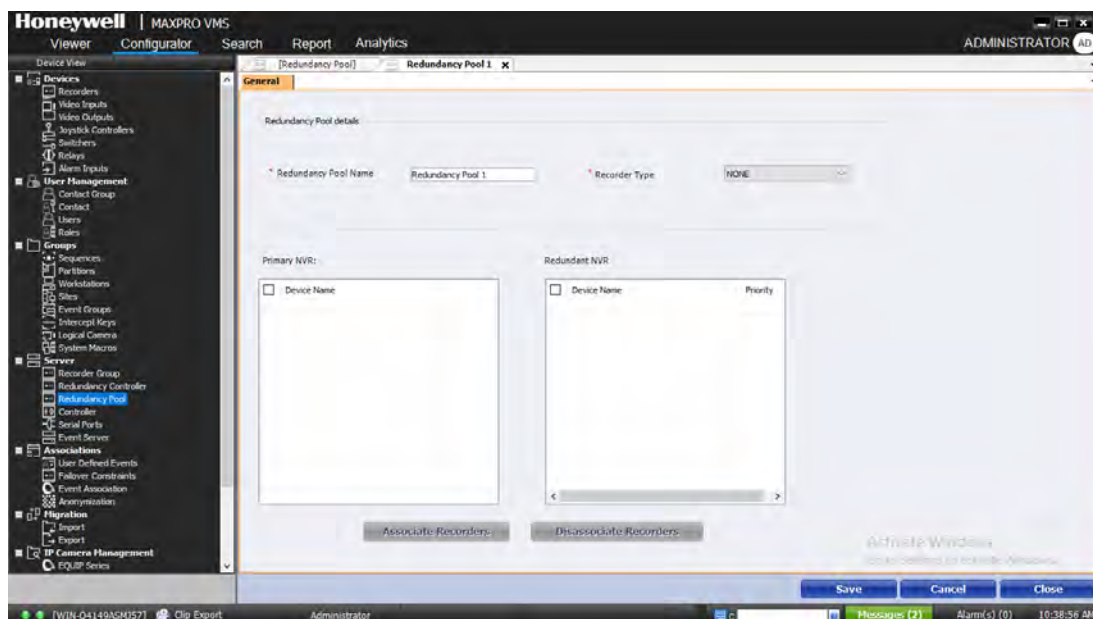


Figure 4-71 Update Redundancy Pool

3. Repeat the step 7 through step 10 of [Configuring Redundancy Pool](#) to associate recorder.
4. Repeat the steps of [Disassociating Recorders from the Redundancy Pool](#) to disassociate recorders.
5. Click Close.

Deleting Redundancy Pool

To delete the Redundancy Pool you need to first disassociate the recorders under that pool. See [Disassociating Recorders from the Redundancy Pool](#).

To delete a Redundancy Pool

1. In the Redundancy Pool screen, select the required Redundancy Pool check box.
2. Click Delete. A confirmation message Do you really want to delete selected Redundancy Pool is displayed.
3. Click Yes to delete.

Trinity Controller

Trinity controller is a service which enables the system to fetch alarm status. It allows you perform PTZ operations and execute the macros. You can edit the special system parameters of the trinity controller. These fields default to values that are satisfactory for most video system applications.

To update the trinity controller

1. Click the Configurator tab.
2. Expand the Servers branch in the navigation area, and then click Controller. The Controller screen appears in the display area.
3. Click Update. The Trinity Controller screen appears.

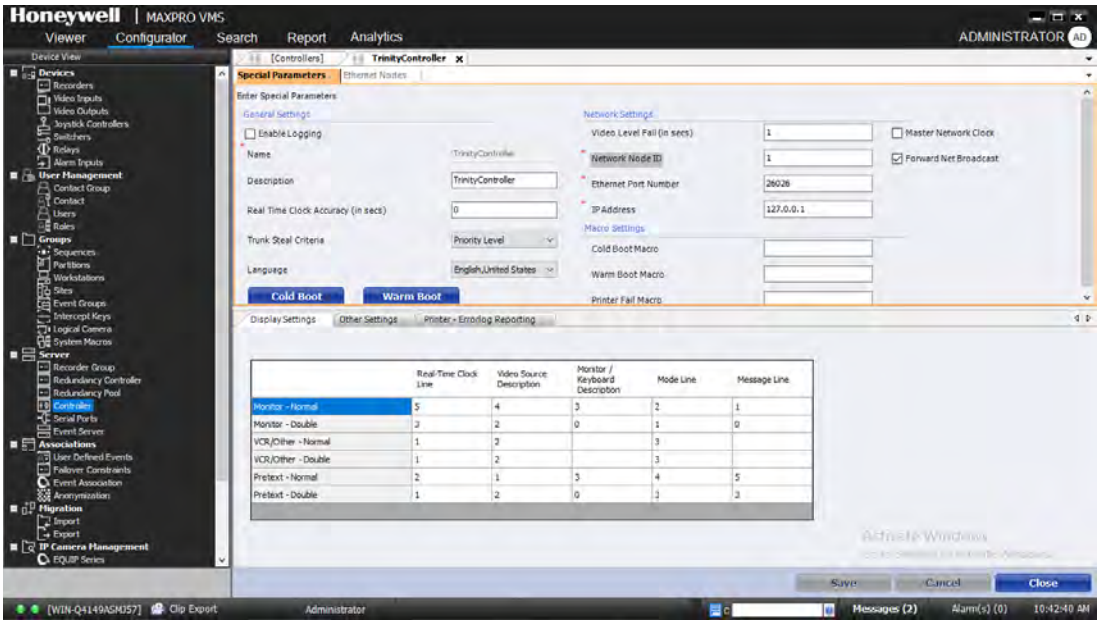


Figure 4-72 Trinity Controller

4. Specify the following settings.
- General Settings

Settings	Instructions/Description
Name	By default, the name of the server, in this case trinity controller appears.
Description	Type a description for the controller.
Real Time Clock Accuracy (in seconds)	Type a value to correct the drift in the real-time clock. After the system is installed and is operational, the number of seconds gained or lost should be measured over a 24-hour period. Type the number of seconds lost or gained in this field. The correction factor is entered using “+” for gained time, and “-” for lost time.

Settings	Instructions/Description
Trunk Steal Criteria	<p>From the drop-down list, select a priority.</p> <p>Priority Level – A user can steal a trunk from another user with a lower priority.</p> <p>On Alarm Only – A trunk can be stolen if an alarm condition causes a system macro to make a video selection. A user cannot steal from another, regardless of priority.</p> <p>Never Steal – Trunks are assigned on a first come first serve basis, regardless of user priorities.</p> <p>Video trunk lines are used for carrying video signals from one system to another. These trunk lines are managed automatically by the MAXPRO VMS to service the video selection demands of the users. It is possible to run out of video trunk lines and the Trunk Steal Criteria allows the selection of the action that occurs under this congestion condition.</p>
Language	From the drop-down list, select the required language.

- Network Settings

Settings	Instructions/Description
Video Level Fail (in seconds)	<p>Type a value to set the detection period time that elapses before a video level failure is reported. Valid values are 0 (immediate) to 30 seconds.</p> <p>A video sync loss is detected immediately and is not effected by the value in the video level fail field.</p>
Network Node ID	<p>Type a unique network node ID.</p> <p>Valid network node numbers are 1 – 99. For a single system this value should be zero (0).</p> <p>The “Network node ID” is not live updated to the server.</p>
Ethernet Port Number	<p>Type the port number that are used by the clients to connect to the server over the Ethernet. The default port number is 26026.</p> <p>The “Ethernet Port Number” is not live updated to the server.</p>
IP Address	Type the IP Address of the server of the Server to which the controller needs to be connected.

- Macro Settings

Settings	Instructions/Description
Cold Boot Macro	<p>Type the desired macro.</p> <p>When the MAXPRO VMS Server is powered up or reset, the Cold Boot macro sequence is executed following all the normal system and equipment initialization.</p> <p>Cold Boot can be initiated from MAXPRO VMS (Cold Boot button in the Trinity Controller page).</p>

Settings	Instructions/Description
Warm Boot Macro	Type the desired macro. When the MAXPRO VMS Server receives a reset command, the Warm Boot macro sequence is executed following all the normal system and equipment initialization. Warm Boot can be initiated from MAXPRO VMS (Cold Boot button in the Trinity Controller page).
Printer Fail Macro	Type the desired macro. When the MAXPRO VMS Server detects the hard-copy printer is no longer online, the Printer Fail Macro sequence is executed.

5. Select the Master Network Clock check box to select this node in a networked system to be the master clock. Selecting this check box ensures that once in every hour, all the other network nodes have the time and date synchronized to this node's clock.

Note: Only one network node in the system is permitted to be the master clock source.

6. Select the Forward Net Broadcast check box to suppress the forwarding of incoming broadcast messages.
7. Specify the settings for the following tabs.
 - Display Settings

Settings	Instructions/Description
Text Type /Height	The rows on the table represent the different text type and heights that can be selected for display. Five (5) lines of normal height text or three (3) lines of double height text can be displayed. <ul style="list-style-type: none"> • Monitor Normal – normal height text displayed on monitors. • Monitor Double – double height text displayed on monitors. • VCR/Other Normal – normal height text displayed on VCRs and other video output devices. • VCR/Other Double – double height test displayed on VCRs and other video output devices. • Pretext Normal – normal height text inserted by pretext subracks. • Pretext Double – double height text inserted by pretext subracks.

Settings	Instructions/Description
Information Lines	<p>The columns on the table represent the types of information that are displayed as text. Not all information line types are available for every text type and height.</p> <ul style="list-style-type: none"> • Real Time Clock Line – defines the line where the Real Time Clock is displayed. • Video Source Description – defines the line where the video input device description is displayed. • Monitor/Keyboard Description – defines the line where the monitor description is displayed. When an operator selects the monitor this text is replaced with Keyboard description or the User description. • Mode Line – defines the line where the mode text (for example, scan mode) is displayed. • Message Line – defines the line where the message line text (for example, warning message) is displayed.

- Other Settings

Settings	Instructions/Description
Auto Message Timeout (in seconds)	Type a value to define the time period for the automatic display of automatic message line text. Valid values are 2-99 seconds.
Pretext Message Timeout (in seconds)	Type a value to define the time period for the automatic display of pretext message line text. Valid values are 2-99 seconds.

Settings	Instructions/Description
Default Test Mode	<p>From the drop-down list, select the required test mode.</p> <ul style="list-style-type: none"> • Normal – displays the system Configuration Summary. • Rx data – displays the data received on all the MAXPRO VMS Server serial communication ports. • TX data – displays the data transmitted from all the MAXPRO VMS Server serial communication ports. • Execute Macros – displays all the macro sequences executed by the system. • Macro Trails – displays the macro trail of the executed macro sequence on the screen. • Error log – displays all the subsequent entries to the error log file on the screen. • Printer – displays all the subsequent output to the hard-copy printer on the screen. • Video Select – displays every video switching action in the system. • Control – displays every control action for PTZ cameras, VCRs and so on. • Auto Number – no data is displayed on the menu output in this test mode. However, if this mode is selected, the description text displayed on video output show the logical device number of the device at the start of the text line. <p>Note: When the system is running, the menu output can be selected to display any of the test modes by selecting ALT-F1 to ALT-F10 on the Qwerty keyboard.</p>
Equipment Polling – Failed Macro	<ul style="list-style-type: none"> • Select an Equipment Polling status. • In the Equipment Fail Macro box, type the desired macro. <p>Types of equipment that can be polled are:</p> <ul style="list-style-type: none"> • Subracks • High Level /Mimic Panels • Keyboards • Network nodes

Settings	Instructions/Description
Pretext Status	<p>Select the required pretext status.</p> <p>Note: All the pretext modules in the system must be of the standard or enhanced type. It is not possible to mix types. This does not apply to post text modules, which are defined, in the video outputs section.</p> <p>You can select the Enhanced Text Card or the Hidden Text Card, but not both. The Shadow and Double Height features can both be selected for either type text card.</p>

- Printer- Errorlog Reporting

Settings	Instructions/Description
Event Group	Type the required event group.
Errorlog Printing	Select Errorlog Printing if you want to send the error log messages to printer.
Sign On/Off	Select Sign On/Off to send a report to printer whenever a user is signed on or signed off.
Errorlog Reporting	Select the type of error log messages that needs to be sent to the printer.

8. Click Save to change the updates.

Cold Boot and Warm Boot

You can perform cold boot or warm boot of the MAXPRO VMS Controller.

1. Click the Configurator tab.
2. Expand the Servers branch in the navigation area, and then click Controller. The Controller screen appears in the display area.
3. Click Update. The Trinity Controller screen appears.
4. Click Cold Boot to restart the MAXPRO VMS Controller.

Or

Click Warm Boot to reinitialize all the devices connected to the MAXPRO VMS without any restart or shutdown of MAXPRO VMS Server.

Serial Port

Serial port is a communication interface with which information is transferred in or out one bit at a time. Serial ports are added to MAXPRO VMS server for communication with joystick controllers (Ultrakey keyboards), Switchers, and Protocol Interface Translators (PIT). You can add up to 20 serial ports in MAXPRO VMS server.

Adding a Serial Port

To add a serial port

- 1. Click the Configurator tab.
- 2. Expand the Servers branch in the navigation area, and then click Serial Ports. The Serial Ports screen appears in the display area.
- 3. Click Add. A Joystick screen appears.

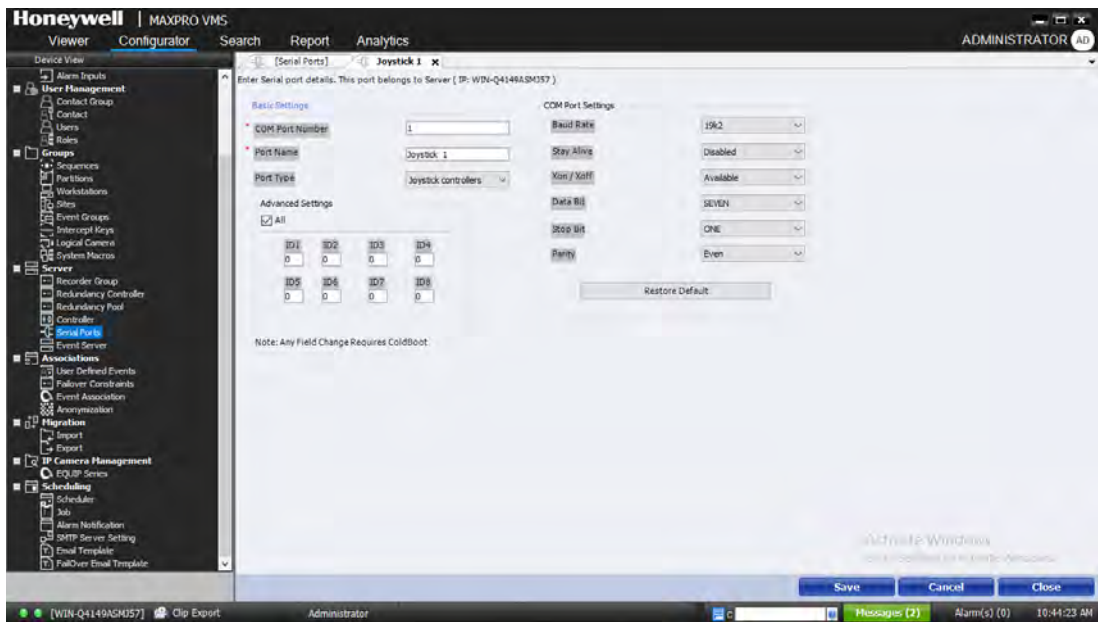


Figure 4-73 Joystick

- 4. Specify the Basic Settings. The following table lists the basic settings.

Field	Description
COM Port Number	The reference number of the serial port. There can be up to 20 ports defined in a single system.
Port Name	The port name that you want to assign. Ensure that the port name does not exceed 18-characters.

Field	Description
Port Type	<p>The type of the serial port. You can select the port type from the drop-down list.</p> <p>The ports types are:</p> <ul style="list-style-type: none"> • Joystick Controller • VB PIT • Auxiliary (Max Pro) • Error log - The error logged in the error log file is sent through the serial port. Only one port can be selected for errorlog data. • Analog -Mimic Panel • Serial Network • Serial Printer - The system hard copy print output is redirected to the serial port if this option is selected. Only one port can be selected as a printer port. • MaxPro Switcher • IO-Control (VideoBlox) • Auxiliary Control (VideoBlox) • Pre-Tilter • Test (Not recommended)

5. Select the Advanced Settings check box, to specify the advance settings. The following table lists the advanced settings.
6. Specify the COM Port Settings. The following table lists the COM port settings.
7. Click Save.

Note: Click Restore Default to restore the default settings.

Updating a Serial Port

You can update the serial port when you want to change the basic, advanced, and COM port settings.

To update a serial port

1. Click the Configurator tab.
2. Expand Server in the navigation area.
3. Click the Serial Ports branch. The serial ports screen appears in the display area.
4. Select the check box corresponding serial port you want to update, and then click Update.
5. Modify the Basic Settings.
6. Modify the Advanced Settings.

Field	Description
ID 1 to ID 8	<p>These fields are used for limiting the amount of data that is transmitted from a selected port. Placing a number in any of these fields only transmits data to the equipment of selected type with that ID number. The ID1 field allows the value ALL to be entered, which enables all data of the selected type to be transmitted, regardless of the ID number. Selecting ALL clears all the other ID fields. The valid ID range for the selected port types are:</p> <ul style="list-style-type: none"> • Keyboard ID 1 – 99 • Subrack ID 1 – 799 • Network ID 1 – 255 • Highlevel/Mimic ID 1 – 99 <p>Enter the value in each ID field and press ENTER. Note: This is not applicable for VideoBlox.</p> <p>For VideoBlox subrack (ID3 – ID4), these two fields represent the video loss source device type.</p> <ul style="list-style-type: none"> • 0 & 0 represents video loss source device is Input cards. • 0 & 1 represents video loss source device is Concentrator. • 1 & 0 represents video loss source device is MVT or pretext devices. • 1 & 1 represents no device as video loss source device. <p>For VideoBlox subrack (ID6), this ID represents the version of matrix switcher hardware for audio switching. 1 represents the old VideoBlox matrix switcher hardware.</p> <p>For VideoBlox subrack (ID7), this ID represents the version of matrix switcher hardware for video switching. 1 represents the old VideoBlox matrix switcher hardware.</p>

Field	Description
Baud Rate	The rate at which data is transferred through the port. By default, a baud rate of 19.2K is available for the port. To change the baud rate, select the desired baud rate from the drop-down list.
Stay Alive	Indicates if the MAXPRO-NET Server is functioning. When you enable this check box, an ACK character is transmitted from the port every 2 seconds. By default, the function is disabled. Select Enabled or Disabled setting from the drop-down list.
Xon/Xoff	If this option is enabled, Xon and Xoff characters are transmitted to resume and stop the data flow (Software handshaking). Xon/Xoff is enabled by default. To change the setting, select the desired setting / from the drop-down list.

Field	Description
Data Bit	The number of data bits per character can be selected as 7 or 8. The default value is 7. To change the data bits setting, select the desired setting from the drop-down list.
Stop Bit	The number of stop bits per character can be selected as 1 or 2. The default value is 1.
Parity	The type of parity to be used by the port can be selected as Even, Odd, or None. The Default is even parity. To change the parity setting, select the desired setting from the drop-down list. The value can also be typed into the field.

7. Modify the COM Port Settings.
8. Click Save.

Deleting a Serial Port

To delete a serial port

1. Click the Configurator tab.
2. Expand Server in the navigation area.
3. Click the Serial Ports branch. The list of existing serial ports is displayed on the screen.
4. Select the check box corresponding to the serial port you want to delete.
5. Click Delete. A message asking for confirmation appears on the top of the display area.
6. Click Yes.

User Defined Events

The devices such as recorders and cameras have predefined events. MAXPRO VMS provides an option to customize new events to recorders and cameras. These events can be mapped to an external source to trigger an alarm whenever an event occurs.

Note: For more information on mapping the events, contact your system administrator.

To add and associate an event to devices

1. Click the Configurator tab.
2. Expand Associations in the navigation area, and then click User Defined Events. The User defined event association screen appears in the display area.
3. Click Add & Associate. The Associated Devices page appears.

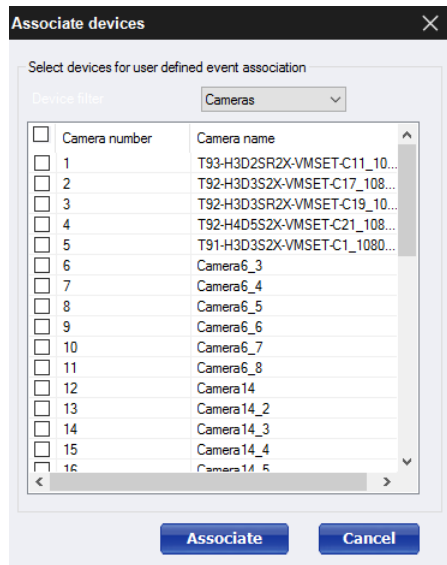


Figure 4-74 Associate Devices

4. From the Device filter drop-down list, select the required device category. The device number and the name of the device are listed.
5. Select the check box corresponding to the name of the device for which you want to define an event, and then click Associate. The device appears on the User defined event association screen.

Note: You can select multiple device names by selecting multiple check boxes.

6. In the Global Event ID box, type the unique global ID. If the Global Event ID is not assigned, MAXPRO VMS assigns a unique global ID automatically when you save the event.
7. In the Event Description box, type a description for the event.
8. In the Start Procedure box, type the required macro to start the event.
9. In the End Procedure box, type the required macro to end the event.
10. Click the Disabled box, and then select True or False from the drop-down list.
11. Click the Severity Level box and edit the severity level.

Note: Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set to 50 on the preferences tab, an alarm is triggered when threshold becomes 51.

12. Click the Normal State box and define the alarm normal state as Closed or Open.
13. Click the Operating Mode box and select the operating mode for the alarm. The available modes are:
 - Direct - The alarm condition activates or de-activates when it physically changes state, or is set or cleared with macros.

- Latched – Once triggered the alarm will remain active until it is reset manually using the alarm clear key on the keyboard.
- Toggle – The first time the alarm is triggered it becomes active, the next time it is cleared.

To add a system generated event

1. Click the Configurator tab.
2. Expand Associations in the navigation area, and then click User Defined Events. The User defined event association screen appears in the display area.
3. Click Add. Follow steps 6 through 11 of See To add and associate an event to devices.

To add Event Groups to events

1. Select the check box corresponding to the device name for which you want to add the Event Group.
2. Double-click the Event Group box. The Select Event Groups page appears.
3. Select the check box corresponding to the Event Group you want to add.
4. Click OK.

Note: You need to add an event group before you associates it to an event. See [Adding an Event Group](#) for more information.

To delete user defined events

1. Click the Configurator tab.
2. Expand the Associations branch in the navigation area, and then click User Defined Events. The User defined event association screen appears in the display area.
3. Select the check box corresponding to the event that you want to delete.
4. Click Delete. A message asking for confirmation appears.
5. Click Yes.

Failover Constraints

Failover Constraints feature enables you to set the constraints for a recorders in case of a failover. It allows you to define set of performance counter rules on a specific site and for the devices under the site. Once the recorder meets the predefined performance rules then the load of the recorder is shifted to another configured recorder automatically without interrupting the surveillance process. You can also set poll intervals to trigger the predefined rules.

The following table explains various constraints available to set the rule:

Constraints Name	Description
CPU	Indicates overall CPU usage of system.
Committed Memory	Committed Memory is the number of bytes that have been allocated by processes, and to which the operating system has committed a RAM page frame or a page slot in the page file (or both). Windows allocates memory for processes in two stages. In the first stage, a series of memory addresses is reserved for a process.
Available Physical Memory	Indicates overall Physical Memory used in percentage
Committed Virtual Memory	Indicates overall Committed Virtual Memory
Virtual Memory can be Committed	Indicates overall Virtual Memory that can be committed
Rate of ReadWrite of Disk	Indicates rate of read and write of disk to resolve hard page faults
Avg Disk Queue Length	Indicates Average queue length Avg Disk Queue Length is one of the main counters in the application. Avg Disk Queue Length is an estimate of requests on the physical or logical disk that are either in service or waiting for service. The value is a product of Disk Transfers/sec (response X I/O) and Avg Disk sec/Transfer.
Disk Write	Indicates overall Disk usage of system
Disk Read	Indicates overall Disk usage of system
Average Disk time read	Indicates average Disk usage of system
Average Disk time write	Indicates average Disk usage of system
Threads in Processor Queue	Indicates overall Disk usage of system Observing Processor Queue Length. A collection of one or more threads that is ready but not able to run on the processor due to another active thread that is currently running is called the processor queue. The clearest symptom of a processor bottleneck is a sustained or recurring queue of more than two threads.
AvailableDiskSpace	Indicates overall disk storage space available in a system in Megabytes
Neo1 Total FPS Received	This is the total FPS received by Neo1. The maximum FPS value that Neo1 should receive is 30. The failover triggers if the disk write value is less than total FPS received.
Neo1 Total BitRate Received	This is the total BitRate received by Neo1

Constraints Name	Description
Neo1 Total FPS Recorded	This is the total FPS recorded by Neo1
Neo1 Total BitRate Recorded	This is the total BitRate recorded by Neo1
Neo1 Total active cameras	Indicates Total active cameras
Neo2 Total FPS Received	Indicates Total FPS Received
Neo2 Total BitRate Received	Indicates Total BitRate Received
Neo2 Total FPS Recorded	Indicates Total FPS Recorded
Neo2 Total BitRate Recorded	Indicates Total BitRate Recorded
Neo2 Total active cameras	Indicates Total active cameras

Configuring the Failover Constraints

To configure the failover constraints:

1. Click the Configurator tab.
2. Expand Associations in the navigation area, and then click Failover Constraints. The Failover Constraints screen appears in the display area.

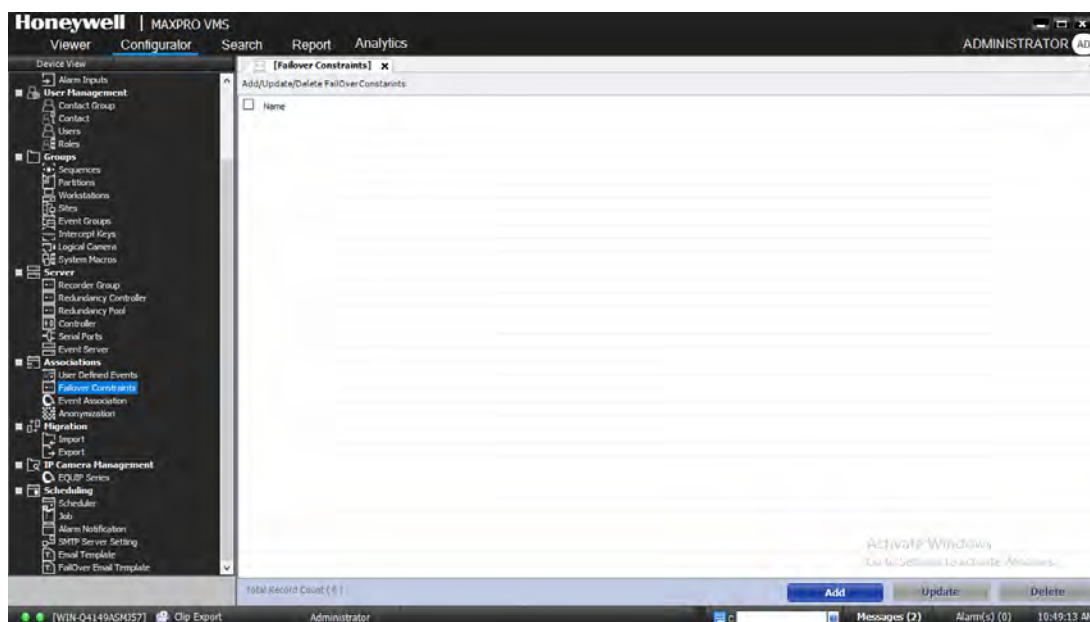


Figure 4-75 Failover Constraints screen

- Click Add. The General settings screen for failover constraints displays.

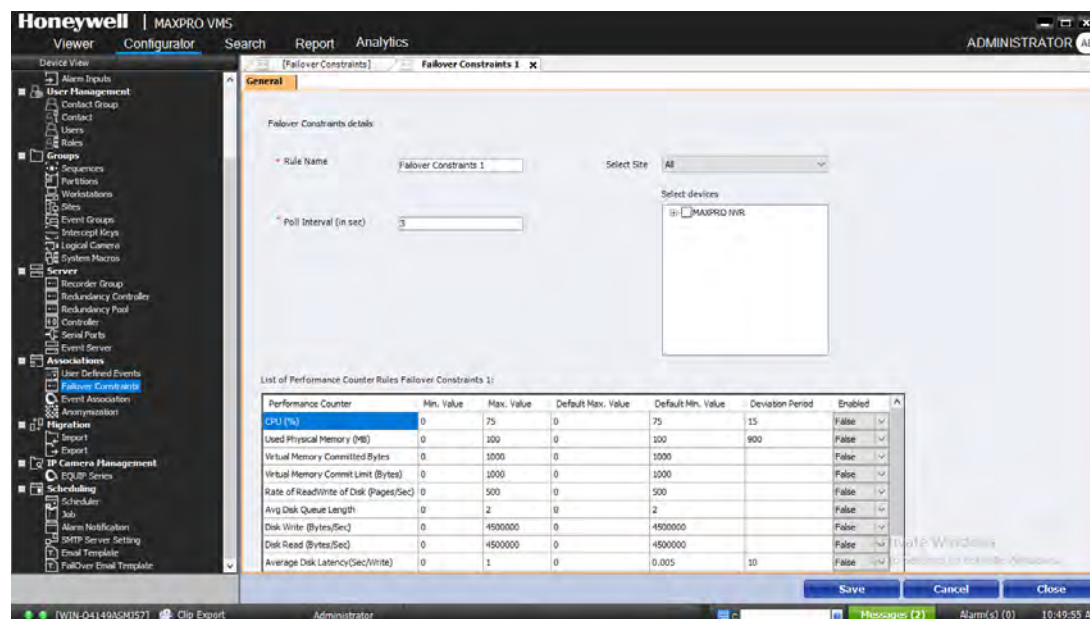


Figure 4-76 Failover Constraints-General Settings

- In the Failover Constraints details box, type a Rule Name.
- In the Select Site drop-down list, select the site for which you want to create a rule.

6. Under Select devices, expand the MAXPRO NVR node and then select the required device. Only MAXPRO NVR devices are supported.

Note: *For a selected recorder, if you set the CPU constraints then only the CPU constraints are assigned to the recorder. Similarly you can assign any number of constraints to the recorder. or you can assign multiple number of constraints to different recorders. The specific constraints assigned are added in corresponding recorder config files.*

7. In the Poll Interval (in Sec) box, type a number to set the poll interval.
8. Under List of Performance Counter Rules, define the rule based on your system and recorder performance and then set the Enable column as True to enable the rule. See [The following table explains various constraints available to set the rule:](#) for detailed explanation.
9. Click Save.

Updating Failover Constraints

To update the Failover Constraints

1. In the Failover Constraints screen, select the required constraint check boxes from the list.
2. Click Update. The General settings screen for Failover Constraints displays.
Or
Double-click the require failover constraint from the list. The General settings screen for specific Failover Constraint is displayed.
3. Repeat the step 4through step 9 of [Configuring the Failover Constraints](#) to update the constraints.
4. Click Close.

Deleting Failover Constraints

To delete a Failover Constraint

1. In the Failover Constraints screen, select the required constraint check box.
2. Click Delete. A confirmation message Do you really want to delete selected Failover Constraint is displayed.
3. Click Yes to delete.

Event Association

The devices such as recorders and cameras have predefined events. MAXPRO VMS provides an option to associate events to a set of cameras and recorders at one stretch with just a few mouse clicks.

Note: *Use this feature to do bulk association of events to a set of cameras and recorders.*

To associate events to cameras and recorders

1. Click the Configurator tab.
2. Expand Associations in the navigation area, and then click Event Association. The Event Association screen appears in the display area.

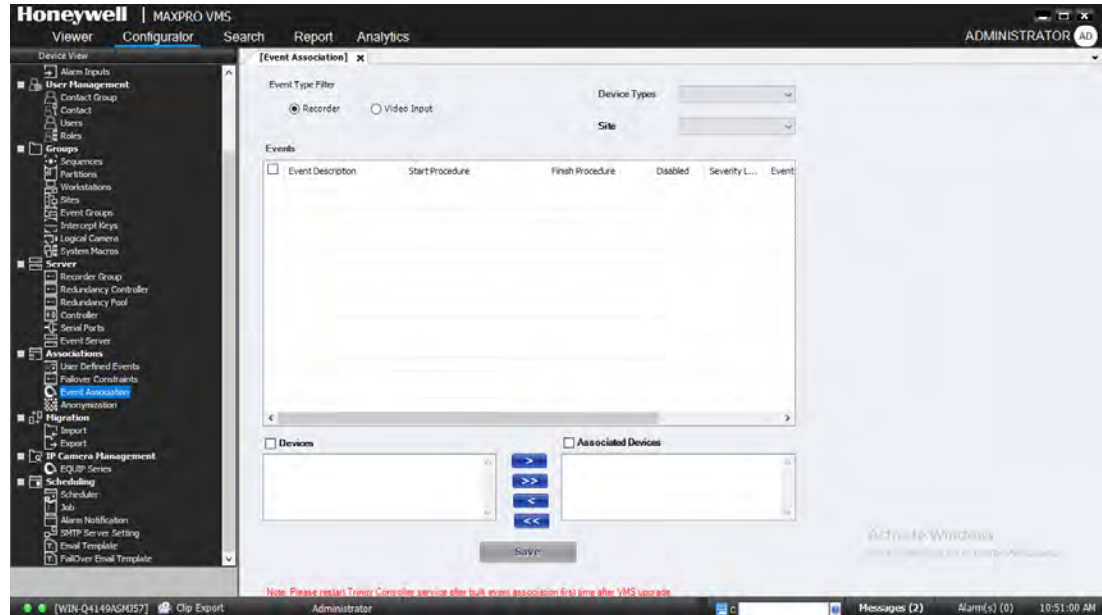






Figure 4-77 Event Association

3. Select “Recorder” or “Video Input” under Event Type Filter.
4. From the Device Types drop-down list, select the required device.

Based on the device selected, the following information appears.

- The list of events associated to a device are listed in the Events table.
 - The number of devices corresponding to the selected device are listed under Devices.
5. From the Site drop-down list, select a site.
 6. In the Events table, select the check box for the events you want to associate to the device. To associate all the events to a device, select the top level check box located in the header section of the Events table.
 7. To complete the device event association, perform the following:
 - To associate one device at a time with the selected events, under Devices, select a camera and then click . The selected camera appears under Associated Devices.
 - Click  to associate all the devices to the selected events. All the devices appear under Associated Devices.

- To remove a device, under Associated List, select a check box corresponding to the device, and then click . The selected device appears under Devices.
 - Click  to disassociate all the devices to Devices.
8. Click Save to save the information.

Anonymization

Anonymization feature is to help the business owner to meet the EU GDPR compliance standards easily. This feature allows user to hide the identifiable personal data in a video surveillance system using masking techniques. This feature is specific to European union region. Only an Administrator can use this feature and grant access. New Equip IP Series cameras are supported by this feature and user can associate the required camera to hide the subject identity. Anonymization is also implemented on HVA streams.

To configure or mask identifiable objects based on the scene environment, see [How to Anonymize objects based on Environment](#) on page 356.

Note: *This feature is license based and it is not supported in Viewer Edition. For R600 Enterprise Edition 60 days of trial license is applicable for both (GDPR) features. For R600 Viewer Edition these features are not available in the permanent demo license.*

User need to associate the required camera and the masking type to view the same in the Viewer. Following are the masking types can be configured to specific cameras.

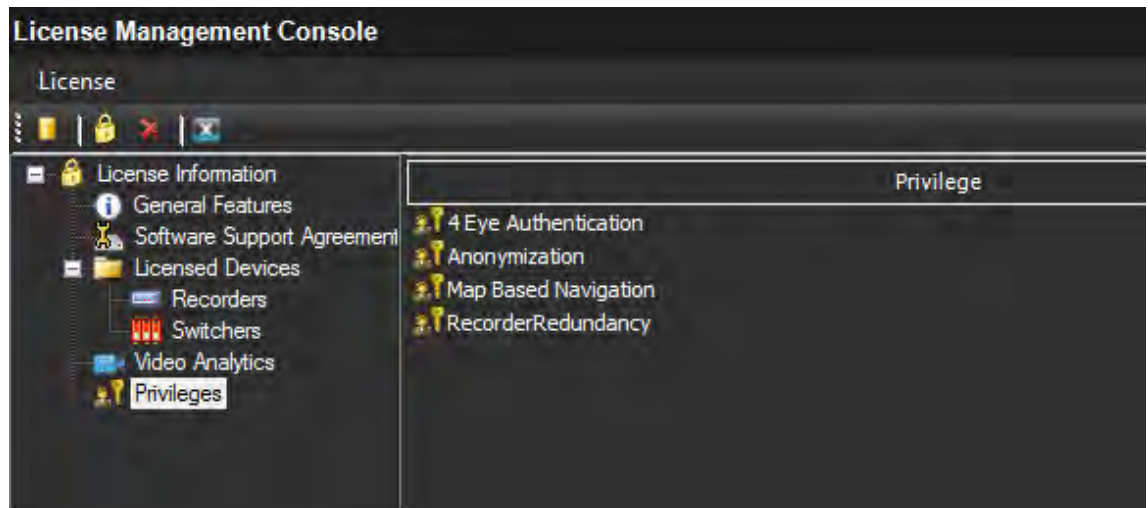
- Blur
- Pixelize

Note: *Only an administrator can access this feature to configure and grant permission to a specific user in User > Privileges screen.*

Licensing

Both Anonymization and Four Eye Authentication (GDPR Favored) features are license based. Contact Honeywell Tech support, see the back cover for contact information.

Once the license is enabled the entries for both the features are displayed in License Management Console > Privileges screen as shown below.

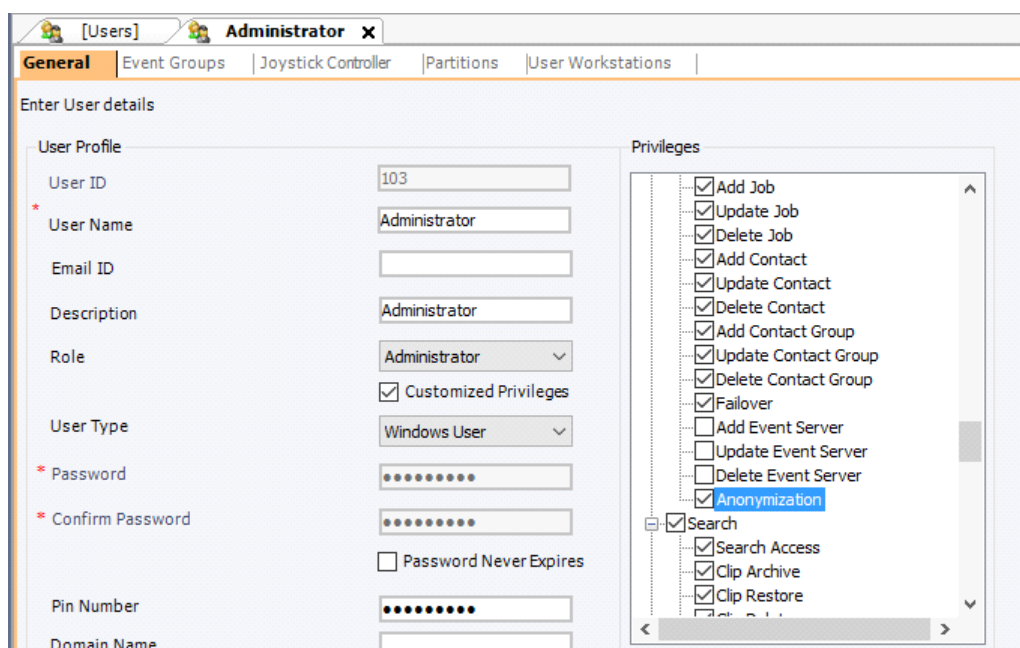


Enabling Anonymization

This option allows user to enable/disable the Anonymization feature in Configurator > Devices View pane. The visibility of the Anonymization option is controlled using this option. By Default only Administrator will have this configuration enabled. Only an Administrator can enable/disable this option for an Operator. To configure or mask identifiable objects based on the scene environment, see [How to Anonymize objects based on Environment](#) on page 356.

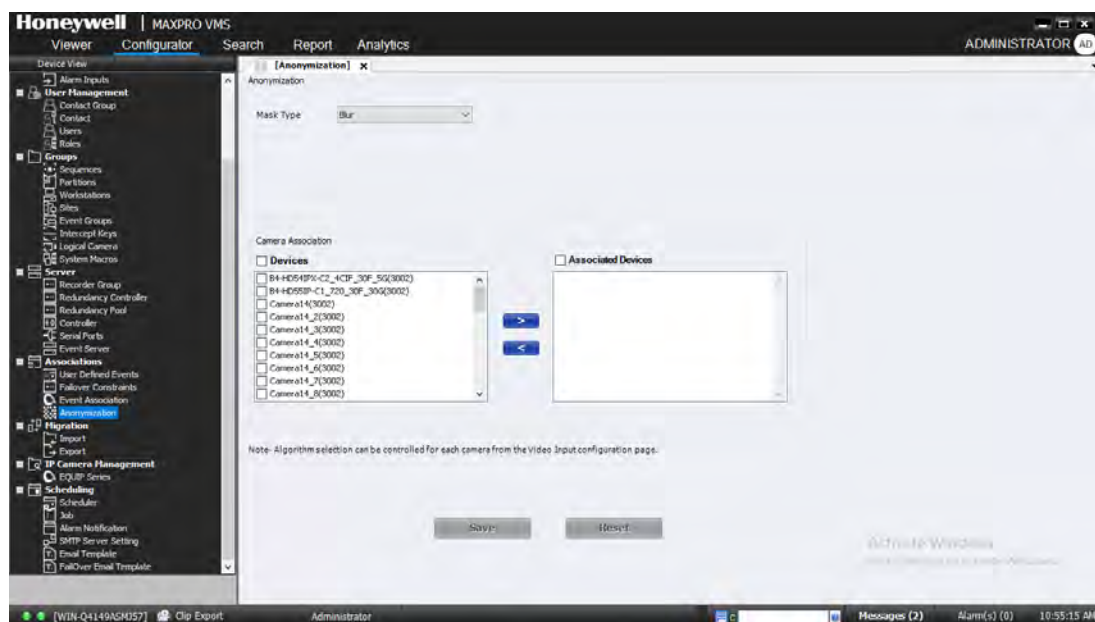
To enable Anonymization feature for a specific user:

1. Perform the steps as explained in [Adding a User](#) section to add a user and privileges.
2. Select the Customized Privileges check box to enable or disable privileges for a user as shown below.
3. Select or clear the Anonymization check box for a specific operator. By default this check box is selected for Administrator user only.





How to configure Anonymization

1. Based on your user privileges if Anonymization is enabled for you then, click the Configurator tab.
2. Expand Associations in the navigation area, and then click Anonymization. The Anonymization screen appears in the display area. By default no cameras are associated for Anonymization



3. From the Mask Type drop down list, select the required option. The available options are
 - Blur: Blurs the Identifiable object.
 - Pixelize: Pixelizes the Identifiable object.
4. Under Camera Association, select the required camera check box in the Devices area.

Tip: To select all the cameras at once, select the Devices check box.

5. To complete the device/camera association, perform the following:
 - To associate one camera at a time, under Devices, select a camera and then click . The selected camera appears under Associated Devices.
 - To remove a camera, under Associated Devices, select a check box corresponding to the camera, and then click . The selected camera appears under Devices. To configure or mask identifiable objects based on the scene environment, see [How to Anonymize objects based on Environment](#) on page 356.
6. Click Save to save the information.
7. Navigate to the Viewer tab, drag and drop the associated camera to view the Anonymization feature.

Viewing Anonymized Video

Ensure that you have associated the required cameras with suitable masking type in the Configurator tab > Anonymization screen. To configure or mask identifiable objects based on the scene environment, see [How to Anonymize objects based on Environment](#) on page 356.

- In the Viewer tab, drag and drop the associated camera on to the panel. The specific camera video with the type of masking is displayed as shown below. The available masking types are
 - Blur: Blurs the Identifiable object
 - Pixelize: Pixelizes the Identifiable object

The following images display the views of maskings:
For Blur



For Pixelize

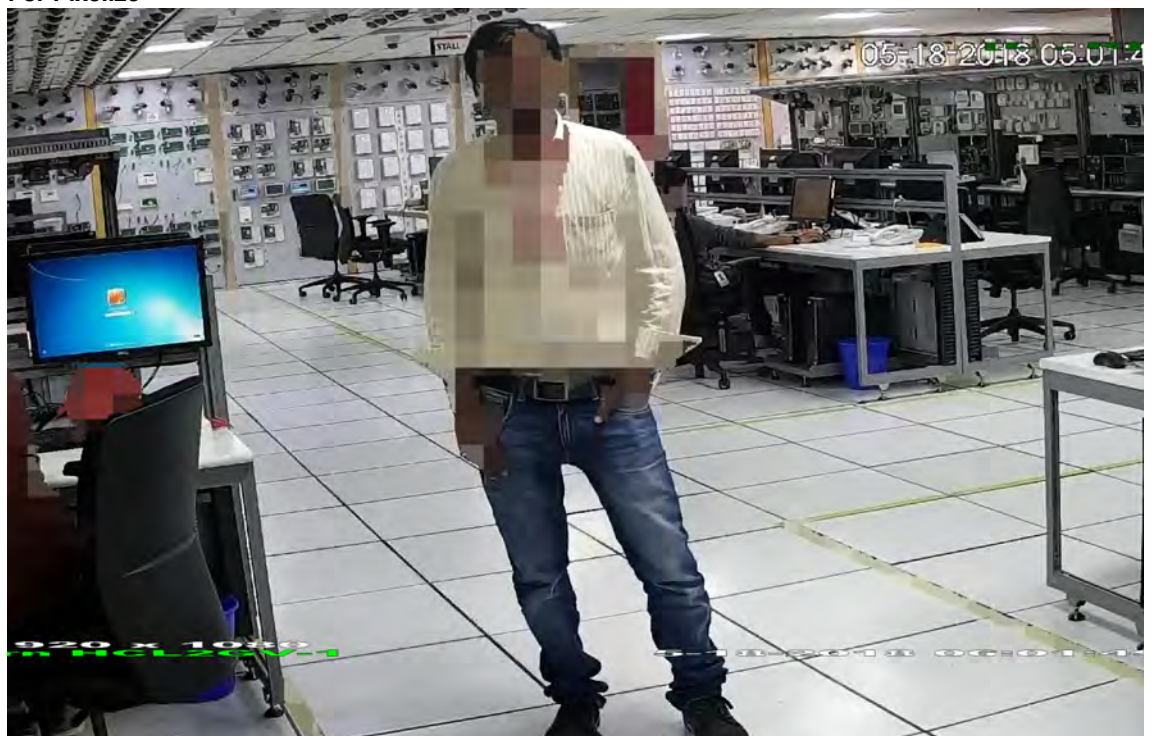


Figure 4-78 Pixelized view

Hide Subject Identity

The new user privilege “Hide Subject Identity” is to control the accessibility to view Anonymized video. This privilege allows the required operator to view the Anonymized video. An Administrator can decide to enable this option to hide the subject identity for a specific Operator. By default this check box is enabled for all the operators.

How to enable Hide Subject Identity Option

1. Perform the steps as explained in [Adding a User](#) section to add a user and privileges.
2. Select the Customized Privileges check box to enable or disable privileges for a user as shown below. Based on the requirement, select or clear the Hide Subject Identity check box for a specific operator. By default the check box is selected for all the users.

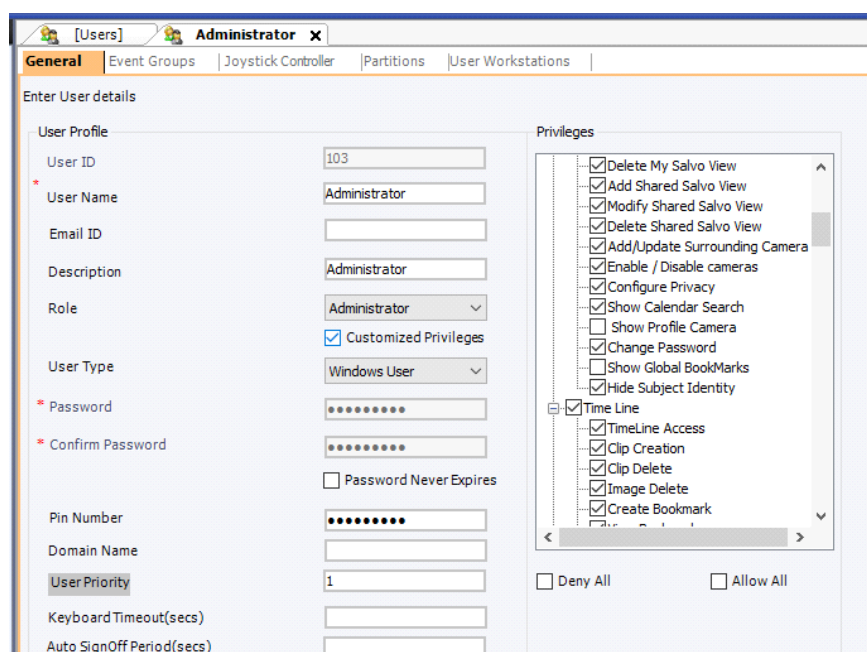


Figure 4-79 Hide Subject Identity

Clip Export Option

Clip export with Anonymization is supported: Anonymization feature is supported in both Playback and Clip Export operation.

Note: If a user exports a clip then only WMV format is supported.

Migration

MAXPRO VMS supports data migration of mpn and max files from legacy applications like MaxproNet. Enterprise NVR configuration data can be migrated into MAXPRO VMS using the HLI file. You can also export the MAXPRO VMS configuration whenever required. From MAXPRO VMS R200 onwards, you can export or import the configuration file of the previous versions of the MAXPRO VMS.

Exporting the Files

To export the database

1. Click the Configurator tab.
2. Expand Migrations in the navigation area, and then click Export. The Export screen appears in the display area.

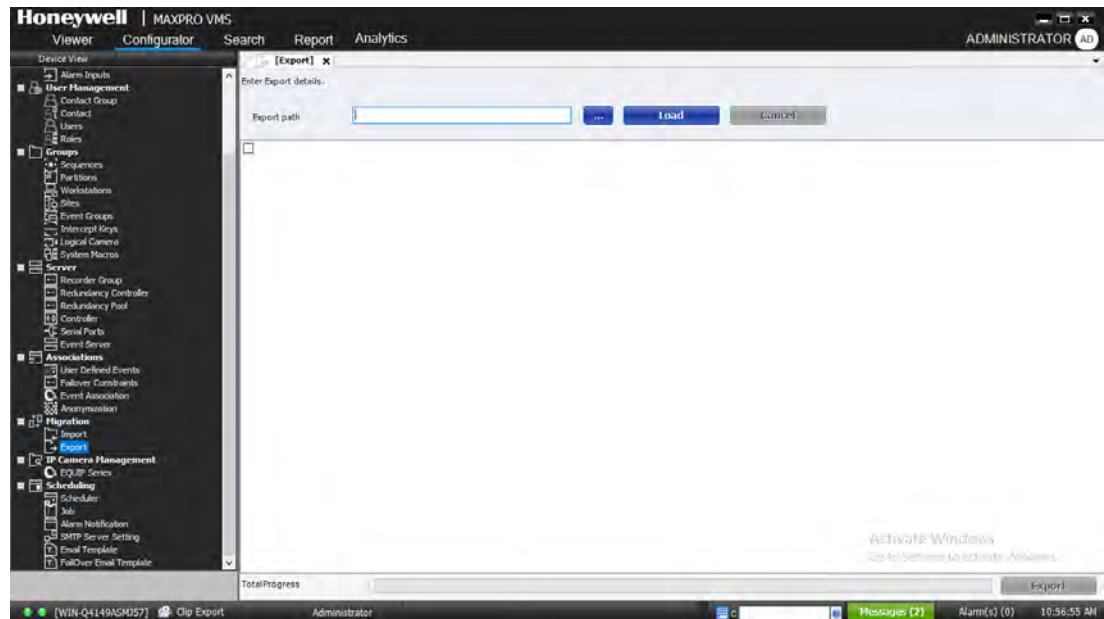


Figure 4-80 Exporting Database

3. In the Export Path box, click the ellipses button to select a path.

Or

If you want to export the files to a network location, click the ellipses button, specify the path, and then click Load.

4. Click Export.

Importing the Database

To import the database

1. Click the Configurator tab.
2. Expand Migrations in the navigation area, and then click Import. The Import screen appears in the display area.

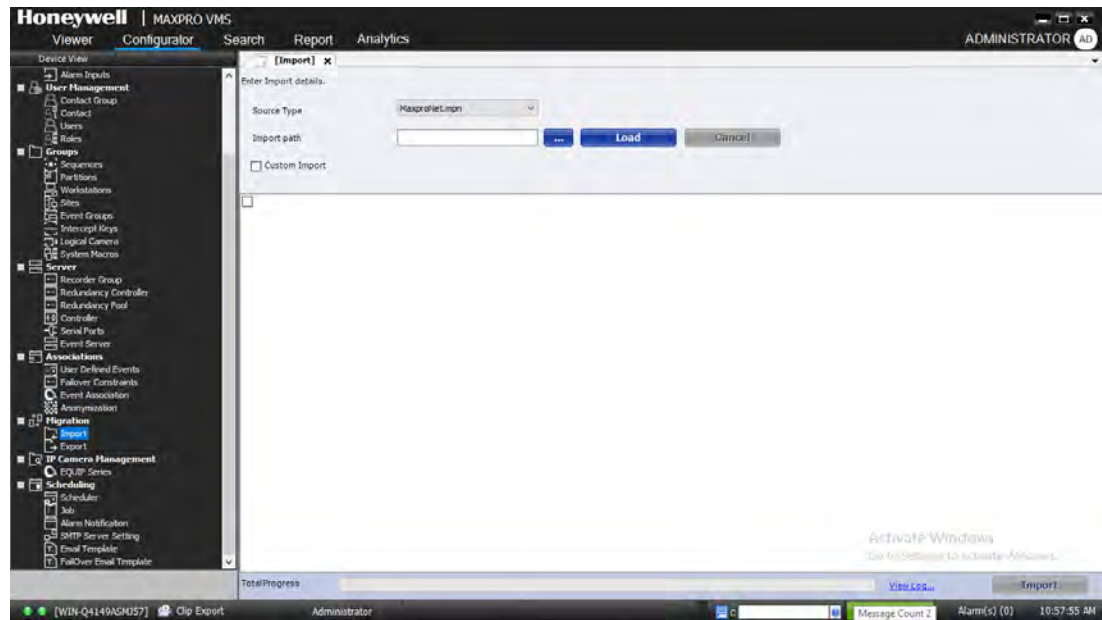


Figure 4-81 Importing Database

3. From the Source Type drop-down list, select the required database type.
4. In the Import Path box, click the ellipses button to select the location.
Or
If you want to import the files to a network location, click the ellipses button, specify the path, and then click Load
5. In the IP Address/ Hostname box, type the IP address or host name of the specific recorder from which mapping has been done in the enterprise HLI file that is being imported.

Note: The IP Address/ Hostname box appears only when you select Enterprise HLI as the source type.

6. Click Import.

Note: When you change the IP address of an recorder, after importing the HLI file, a confirmation message is displayed and prompts you to delete sub devices. If you click Yes, the hybrid cameras revert to analog cameras. The VCR entries are missed and hence, you have to import .mpn and .ini file once again to retain the settings of MaxproNet and HLI. However, the Digital Input Trunk remains unchanged. If you click No, the settings of hybrid camera does not change. It is recommended to click No when the message asking for confirmation appears to deflect sub devices.

Equip Series Camera

You can upgrade, assign a new IP, and also check the version details of the Equip series cameras that are connected to MAXPRO VMS.

To discover Equip series cameras

1. Click the Configurator tab.
2. Expand IP Camera Management in the navigation area, and then click Equip Series. The Equip Series screen appears in the display area displaying the list of discovered cameras by the system.

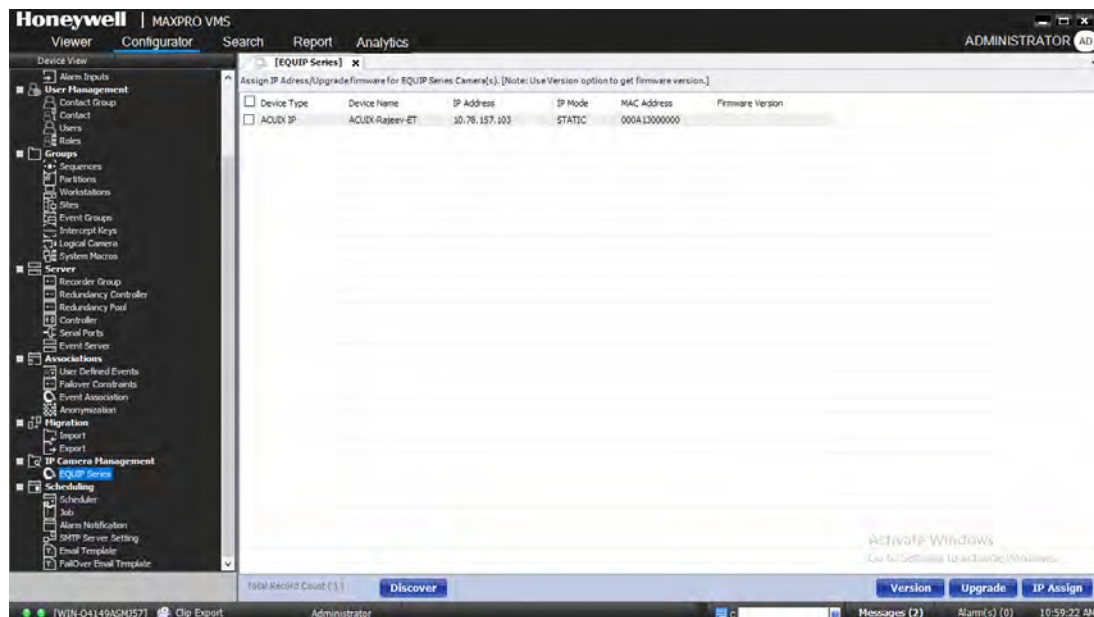


Figure 4-82 Equip Series Cameras

Version

To check the version

1. Click the Configurator tab.
2. Expand IP Camera Management in the navigation area, and then click Equip Series. The Equip Series screen appears in the display area.
3. Select the check box corresponding to the cameras for which you want to check version.
4. Click Version.

Firmware Upgrade

To upgrade the firmware

1. Click the Configurator tab.
2. Expand IP Camera Management in the navigation area, and then click Equip Series. The Equip Series screen appears in the display area.
3. Click Upgrade. The upgrade options appear in the lower pane.

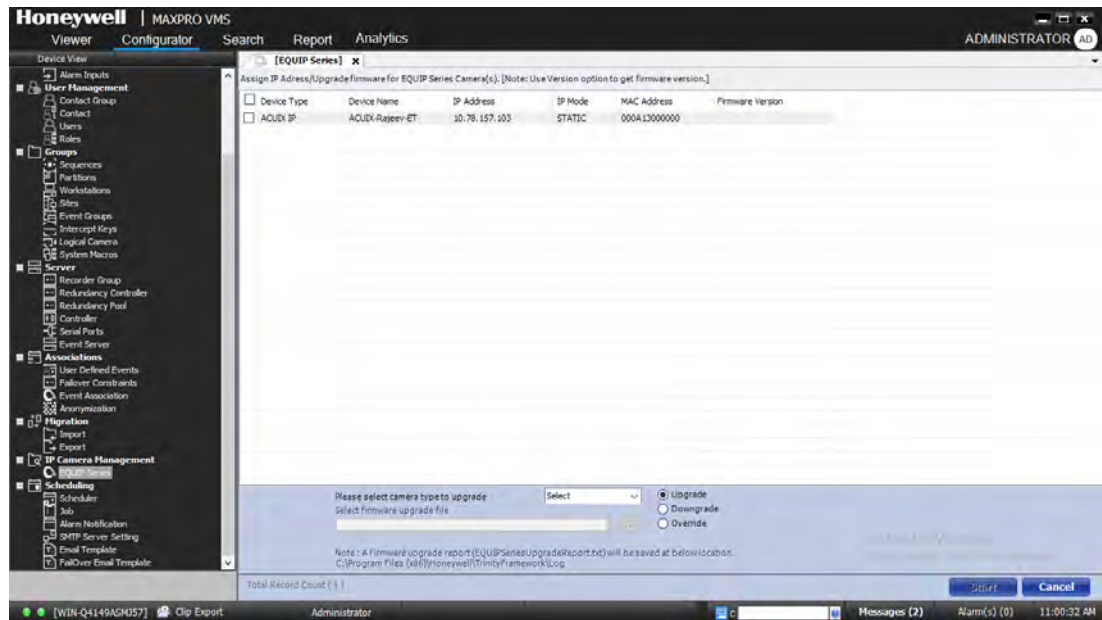


Figure 4-83 Upgrade Options

4. From the Please select camera type to upgrade drop-down list, select the required Equip series camera. The available cameras for the Equip series are displayed.
5. Select the check box corresponding to the cameras that you want to upgrade firmware.
6. In the Select firmware upgrade file box, click the ellipses button, and then select the firmware upgrade file.
7. Click Start. A confirmation message appears.
8. Click OK.

Assigning IP Address

To assign IP address

1. Click the Configurator tab.
2. Expand IP Camera Management in the navigation area, and then click Equip Series. The Equip Series screen appears in the display area.
3. Select the check box corresponding to the cameras for which you want to assign IP address.
4. Click IP Assign. The IP assign options appear in the lower pane.

5. In the Enter Starting IP Address box, type the starting IP address for the camera. The next available IP address from the one that is entered is assigned to cameras that are selected.
6. In the Subnet Mask box, type the subnet mask for the camera.
7. In the Default Gateway box, type the default gateway for the camera.
8. Click Start.

Automatically Obtaining IP address for a Camera

To obtain an IP address

1. Click the Configurator tab.
2. Expand IP Camera Management in the navigation area, and then click Equip Series. The Equip Series screen appears in the display area.
3. Double-click the camera for which you want to obtain an IP address. The general settings for the camera appear.

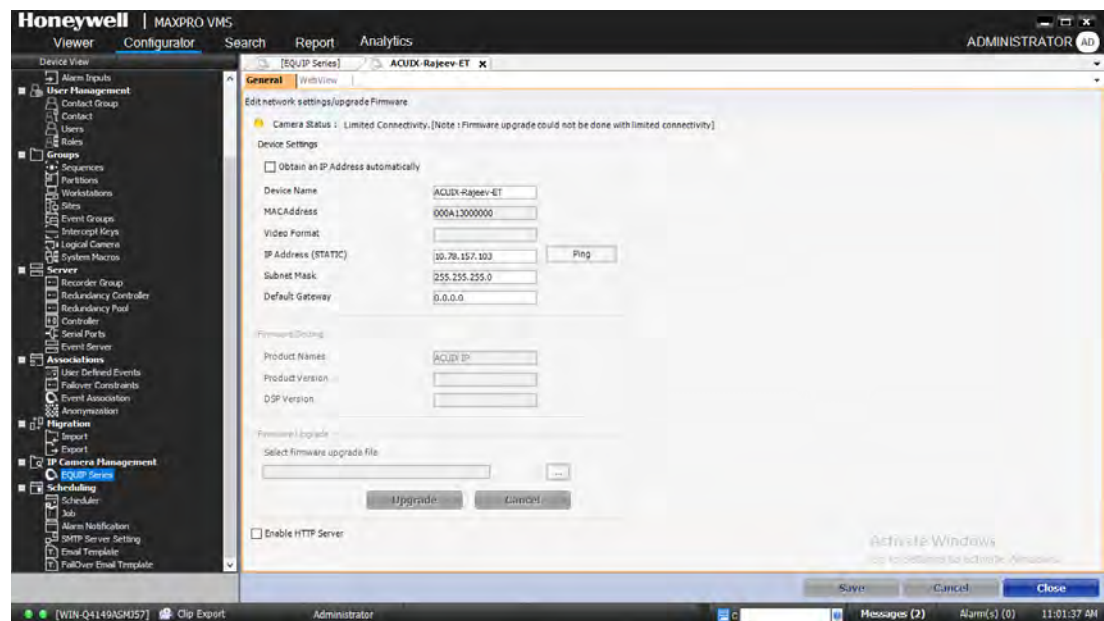


Figure 4-84 Camera General Settings

4. Select the Obtain an IP Address automatically check box, and then click Save. A confirmation message appears.
5. Click OK.

Note: You can also edit the IP address, subnet mask, and default gateway if the camera has a static IP address.

Scheduler

You can create jobs in MAXPRO VMS to back up data and also to clean up the database. You can associate these jobs to schedulers. MAXPRO VMS currently has a default scheduler and it is recommended to retain the default settings.

Updating a Scheduler

To update a scheduler

1. Click the Configurator tab.
2. Expand Scheduling in the navigation area, and then click Scheduler. The Scheduler screen appears in the display area.
3. Click Update. The Scheduler General Settings screen appears.

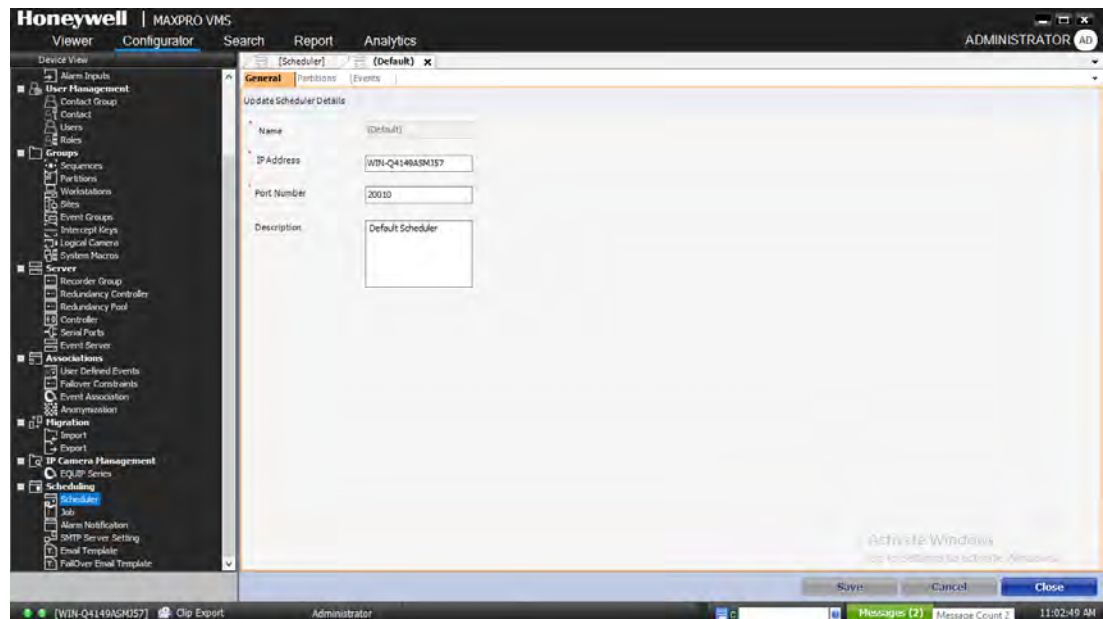


Figure 4-85 Scheduler General Settings

4. In the IP Address box, the default IP address displays. You can type a new IP address as applicable.
5. In the Port Number box, the default port number displays. You can type a new port number as applicable.
6. In the Description box, the default description displays. You can type a new description for the scheduler as applicable.
7. Associate Partitions. See [Associating Partitions to Scheduler](#) for more information.
8. Associate Events. [Associating Events and Event Attributes to a Scheduler](#) for more information.
9. Click Save.

Associating Events and Event Attributes to a Scheduler

You can associate one or more events to the scheduler. An alarm is triggered whenever any of the associated event occurs for the scheduler. For certain events, you can also associate event attributes. For example, for an Scheduler Job Failed event, you can associate attributes such as Scheduler Name, Scheduler Description and so on. For every attribute that you associate, you can set a value based on which the event is triggered. In the above example, you can associate the attribute Scheduler Name to the event and set its value as Scheduler A. When this event is associated to the scheduler, an alarm is raised when the event “Scheduler Job Failed” occurs for the Scheduler Name “Scheduler A”.

To associate events to a scheduler

1. Click the Events tab. The screen displays the associated events, if any.

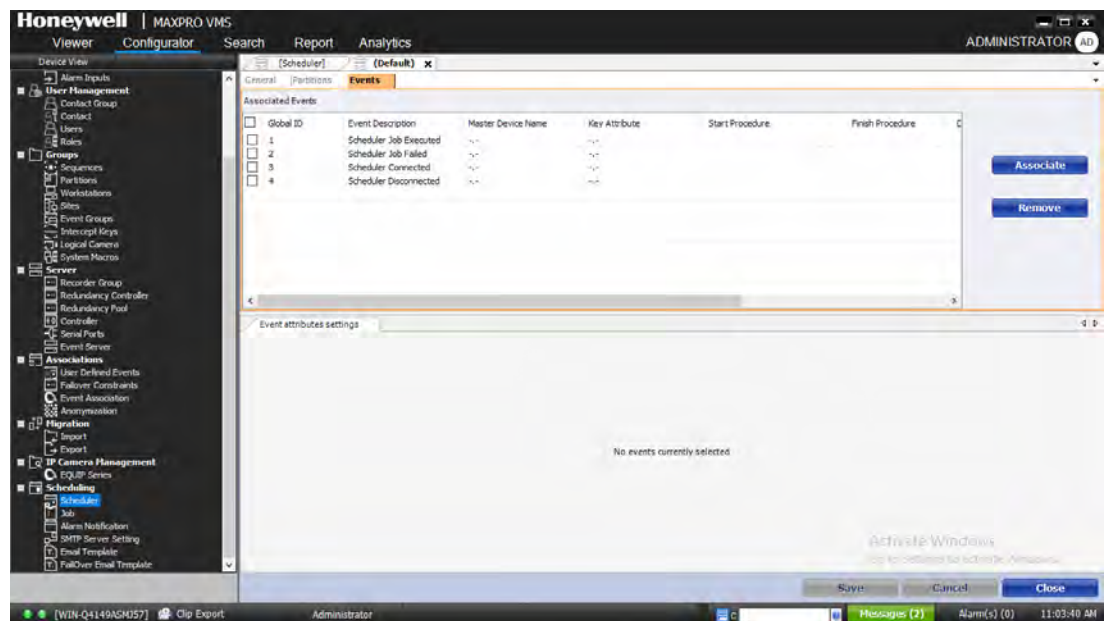


Figure 4-86 Scheduler Events

2. Click Associate. The Select From List page appears.
3. Select the check box corresponding to the event you want to associate.
4. Click OK.

To disassociate events from a scheduler

- Select the check box corresponding to the event, and then click Remove. The events are disassociated from the scheduler

To add Event Groups to events

1. Select the check box corresponding to the event you want to add the Event Group.
2. Double-click on the Event Group box. The Select Event Groups page appears.

3. Click the check box corresponding to the Event Group you want to add.
4. Click OK.

Note: You need to add an event group before you associates it to an event. See [Adding an Event Group](#) for more information.

To disable an event

1. Select the check box corresponding to the event you want to disable.
2. Click on the Disabled box. A drop-down list is enabled.
3. Select True to disable the event.

To assign severity level

1. Select the check box corresponding to the event you want to assign the severity level.
2. Double-click on the Severity Level box and edit the severity level.

Note: Severity level is set to trigger alarms when the threshold is met. For example, if the threshold is set 50 in the preferences tab, an alarm is triggered when threshold becomes 51.

To enter remarks

1. Select the check box corresponding to the event you want to enter remarks.
2. Click the Remarks box and type the remarks

To assign macros

1. Select the check box corresponding to the event you want to assign macros.
2. Click the Start Procedure box, and then type the required macro.
3. Click the End Procedure box, and then type the required macro.

Associating Event Attributes

Before you begin

- Associate events.

To associate event attributes

1. Select the check box corresponding to the event for which you want to associate event attributes. The Event attributes settings appear in the lower pane.
2. Click Associate. The Select Available Event Attributes page appears.
3. Select the check box corresponding to the event attributes that you want to associate.
4. Click OK.

To disassociate event attributes from a video input

- Select the check box corresponding to the event attribute, and then click Remove.

Associating Partitions to Scheduler

You can associate partitions to a scheduler. Associating a partition to a scheduler restricts a non-associated user of the partition from viewing the scheduler or changing the settings of the scheduler.

You can associate more than one partition to a scheduler.

Before you begin

- Add a Partition. See [Adding a Partition](#) for more information.

To associate partitions to a scheduler

1. Click the Partitions tab. The screen displays the associated partitions, if any.

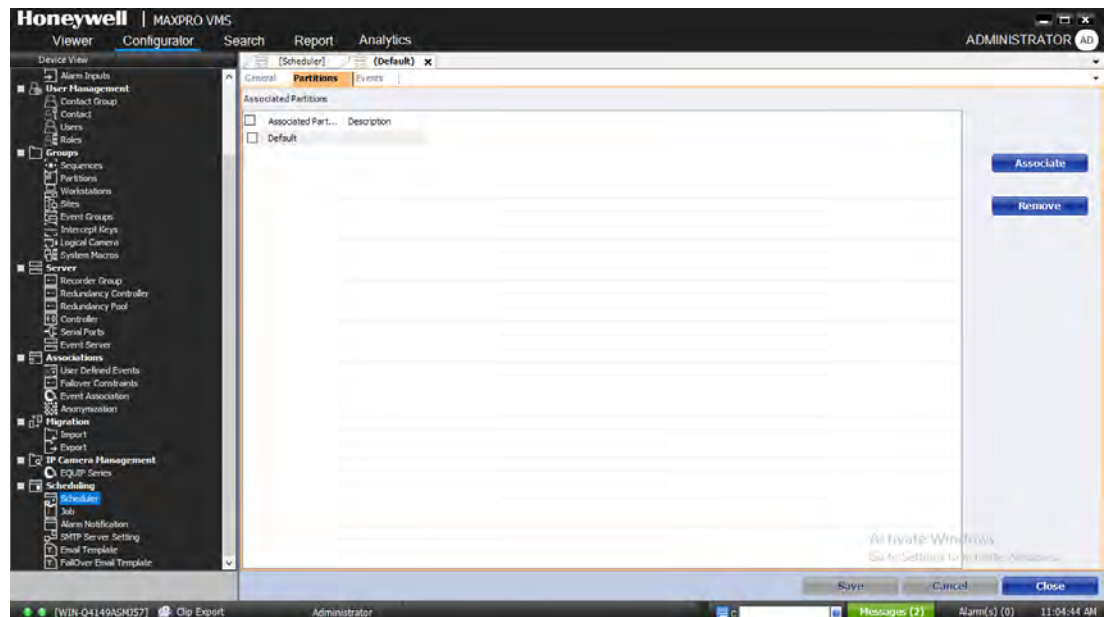


Figure 4-87 Scheduler Partitions

2. Click Associate. The Select Partitions page appears.
3. Select the check box corresponding to the partition name you want to associate.
4. Click OK.

To disassociate partitions from a scheduler

- Select the check box corresponding to the partition name, and then click Remove.

Jobs

Jobs are tasks that are automatically executed at a stipulated time and date. Jobs can be scheduled to clean up database and back up the database. The frequency to perform the tasks can be defined. Only a user with admin rights can create jobs in MAXPRO VMS.

Adding Jobs

You can add a job to clean up the database or backup the data.

To add a job

1. Click the Configurator tab.
2. Expand Scheduling in the navigation area, and then click Job. The Job screen appears in the display area.
3. Click Add. The Schedule Job screen appears.

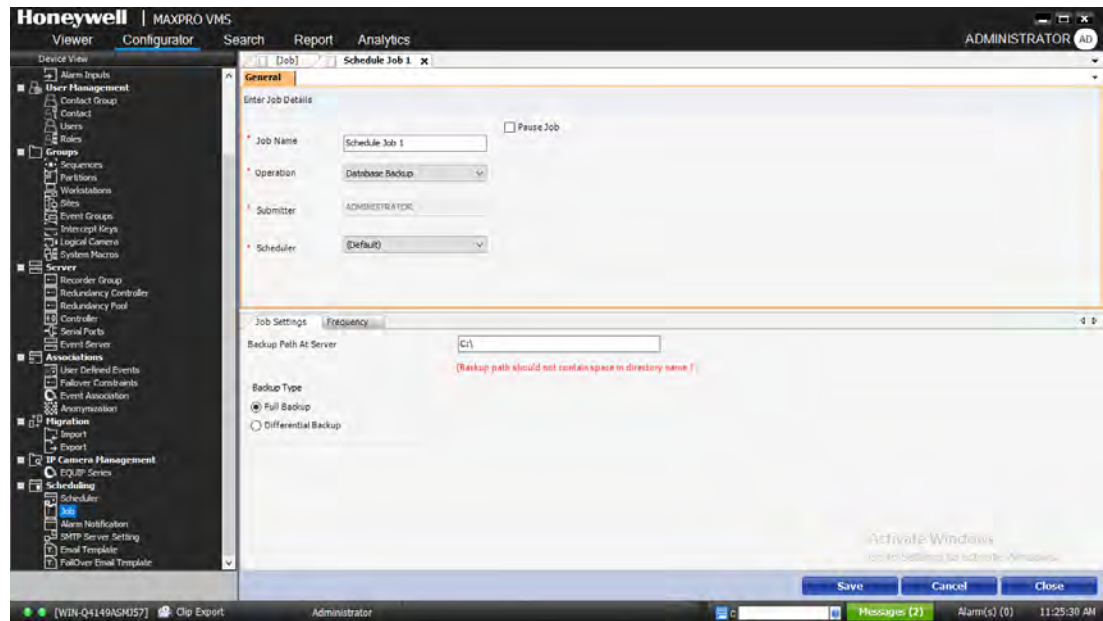


Figure 4-88 Schedule Job

4. In the Job Name box, type the name for the job.
5. From the Operation drop-down list, select Database Cleanup or Database Backup.
6. From the Scheduler drop-down list, select the required scheduler.
7. On the Job Settings tab, specify the settings. The following table lists the settings for both Database Cleanup and Database Backup
8. On the Frequency tab, specify the following settings.

Settings	Instructions
Database Backup	<ul style="list-style-type: none"> In the Backup Path At Server box, type the path to back up the data. <p>Note: The backup path must not contain any spaces in the directory name.</p> <ul style="list-style-type: none"> In the Backup Type section, click Full Backup or Differential Backup as per your requirement. <p>Note: Differential backup contains all files changed since the last full backup. Ensure that a full back up is taken at least once before the differential back.</p>
Database Cleanup	<ul style="list-style-type: none"> Select Event History or Audit Log or both as per the requirement. In the Cleanup Criteria, select All if you want to clean up all records in the database. <p>or</p> <ul style="list-style-type: none"> Select Last, and then type the number of days from when the records should be cleaned. For example, if you type 30, then the records of the last 30 days are cleaned. <p>or</p> <ul style="list-style-type: none"> Select Last, and then type the number of records to be cleaned. For example, if you type 30, then the last 30 records that were created are deleted.

Settings	Instructions
Start From	Specify the start date and time.
End By	Specify the end date and time.
No End Date	Select this option if you do not want any end date for any schedules.
Frequency	<p>You can choose from a set of frequencies that are available. The available frequencies are:</p> <ul style="list-style-type: none"> Now - to run a job at that point of time. Once - to run a job once. Hourly - to run a job every hour. Daily - to run a job daily. Weekly - to run a job weekly. Select a day on which you want the job to run. Monthly - to run a job monthly. In the Every__of every__Month(s), type the day on which the job has to be performed every month. Yearly - to run a job yearly.

9. Click Save.

Alarm Notification

The alarms that are triggered can be notified to users. You can select a device, its events, and associate it to a contact group. The users belonging to the contact group receive a notification whenever a selected event occurs and an alarm is triggered.

To configure an alarm notification

1. Click the Configurator tab.
2. Expand Scheduling in the navigation area, and then click Alarm Notification. The Alarm Notification screen appears.

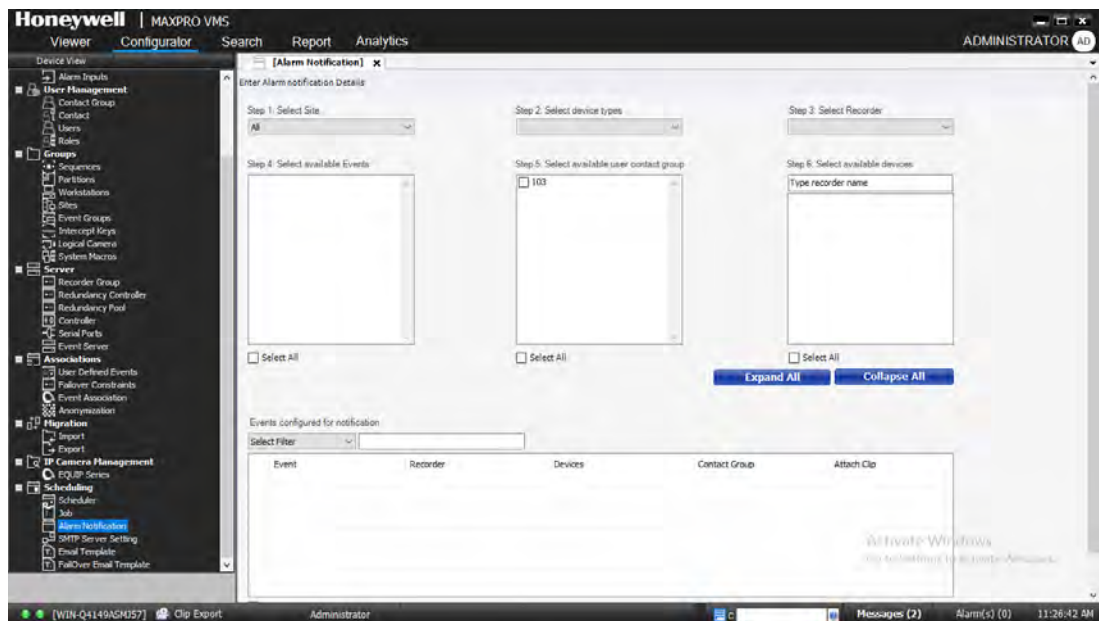


Figure 4-89 Alarm Notification

3. From the Step 1: Select Site drop-down list, select required site.
4. From the Step 2: Select device types drop-down list, select the required device type. The related devices, the associated events, the available user contact group and the available devices are displayed.
5. In the Step 3: Select Analytics Server, select the required analytics server.
6. In the Step 4: Select available Events, select the required events. If you want to select all the events, click Select All.
7. In the Step 5: Select available user contact group, select the contact group check box for which the alarm notification needs to be sent. If you want to select all the user contact groups, click Select All.
8. In the Step 6: Select available devices, select the required available devices check box. You can click Expand All to expand the devices tree. Similarly you can click Collapse All to collapse the devices tree.
If you want to select all the available devices, click Select All.

- Click Save. The selected events for which alarm notification needs to be sent is displayed in the Events Configured for notification section as shown below.

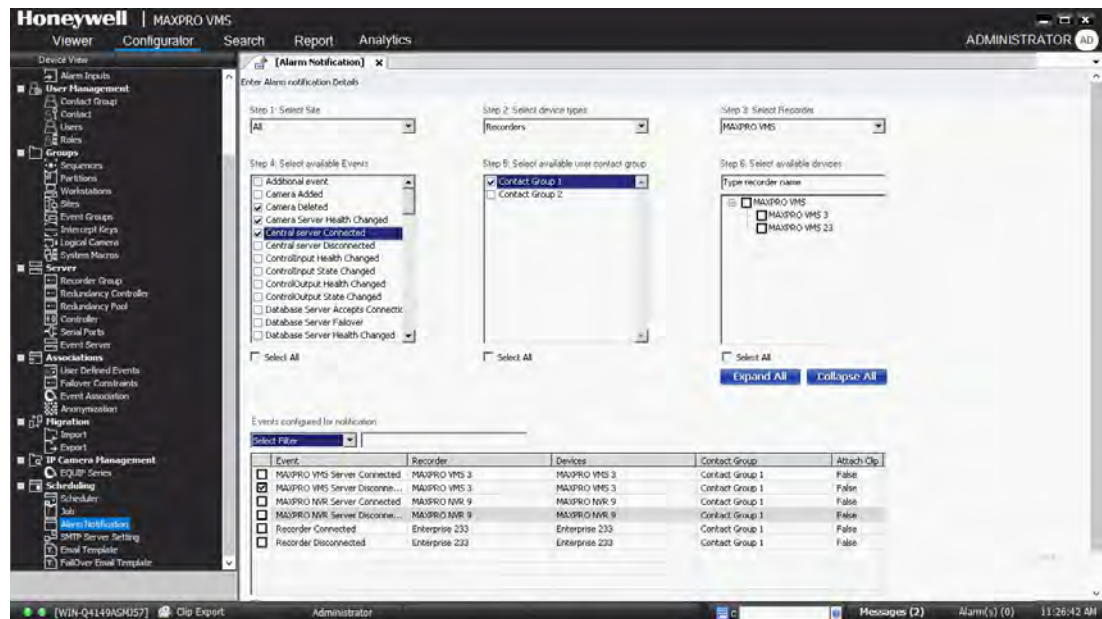


Figure 4-90 Events Configured for notification

Removing events from alarm notification

- In the Events Configured for notification section, select the required events.
- Click Remove.

Controlling Alarm/Message Flashing

User can disable/enable the continuous alarm/message flashing for a workstation in the VMS application.

To enable/disable alarm flashing/blink

- Navigate to the Bin folder and then locate MmShell.exe.config file.
- Open the config file using Notepad.
- Locate the below parameters and change the value to False or True for alarm blink and message blink accordingly.

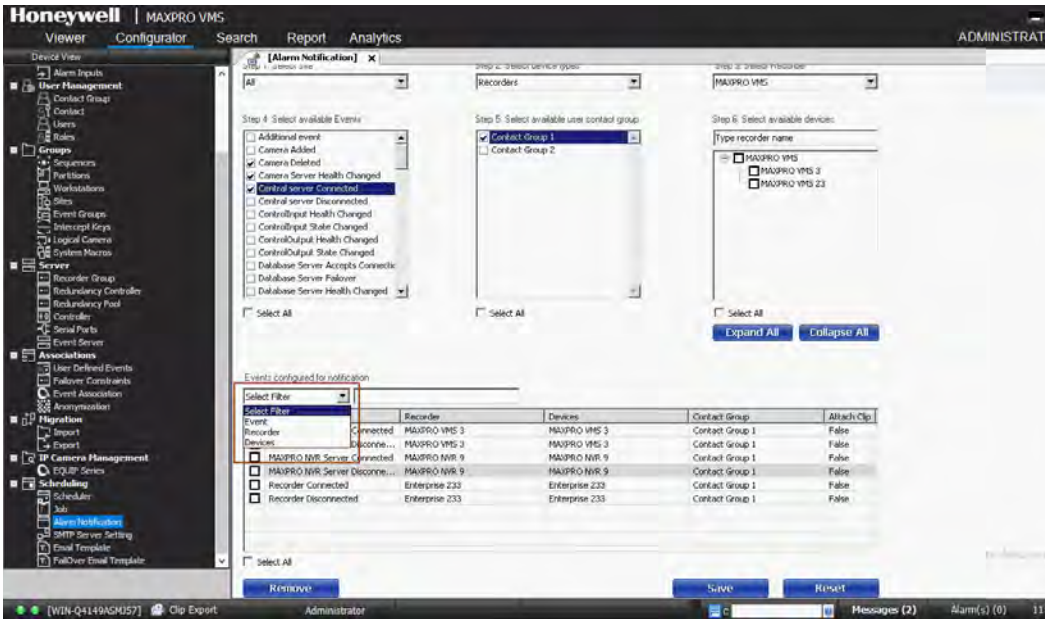
Note: Alarm blink is disabled or set to False by default.

- <add key="AlarmBlink" value="False" />
- <add key="MessageBlink" value="True" />

Filtering the Events Configured

To filter the events configured

- 1. In the Events Configured for Notification, select the filter from the drop down list as shown below.
Or
Type the filter name in the box. The specified events are displayed in the table.



- 2. Click Save.

Attaching Clip

You can attach a clip to the event configured for the notification.

To attach a clip to an event

1. In the Events Configured for Notification table, double-click on the required event under Attach Clip as shown below. A drop-down list is displayed

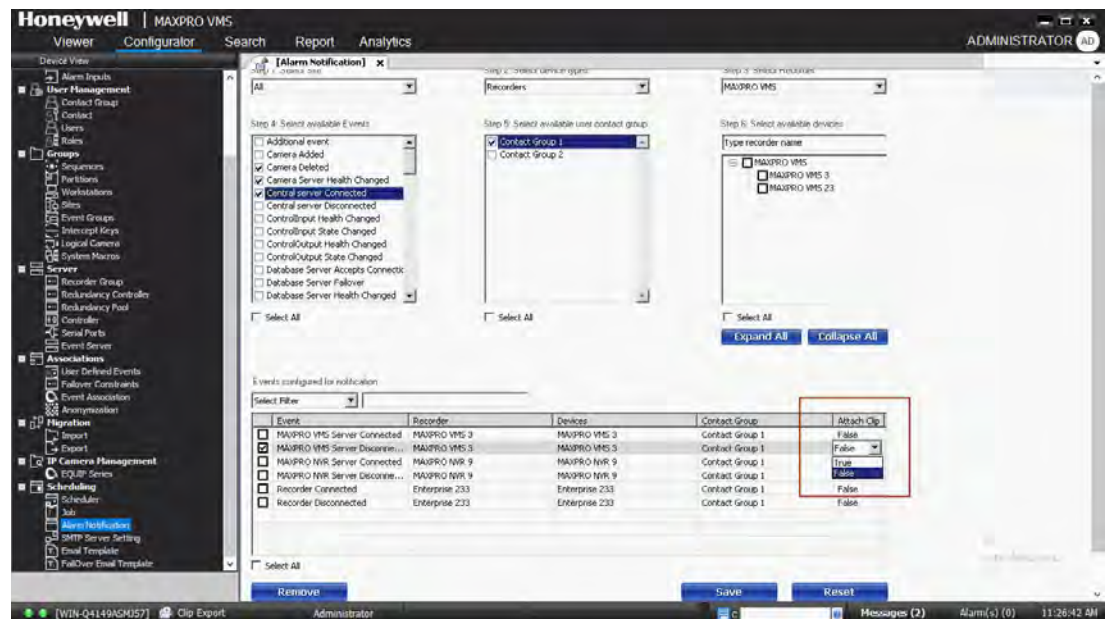


Figure 4-91 Attaching Clip

2. Select True to attach the clip and then click Save.

SMTP Server Settings

To configure SMTP settings

1. Click the Configurator tab.
2. Expand Scheduling in the navigation area, and then click SMTP Server Setting. The SMTP Server Settings screen appears in the display area.

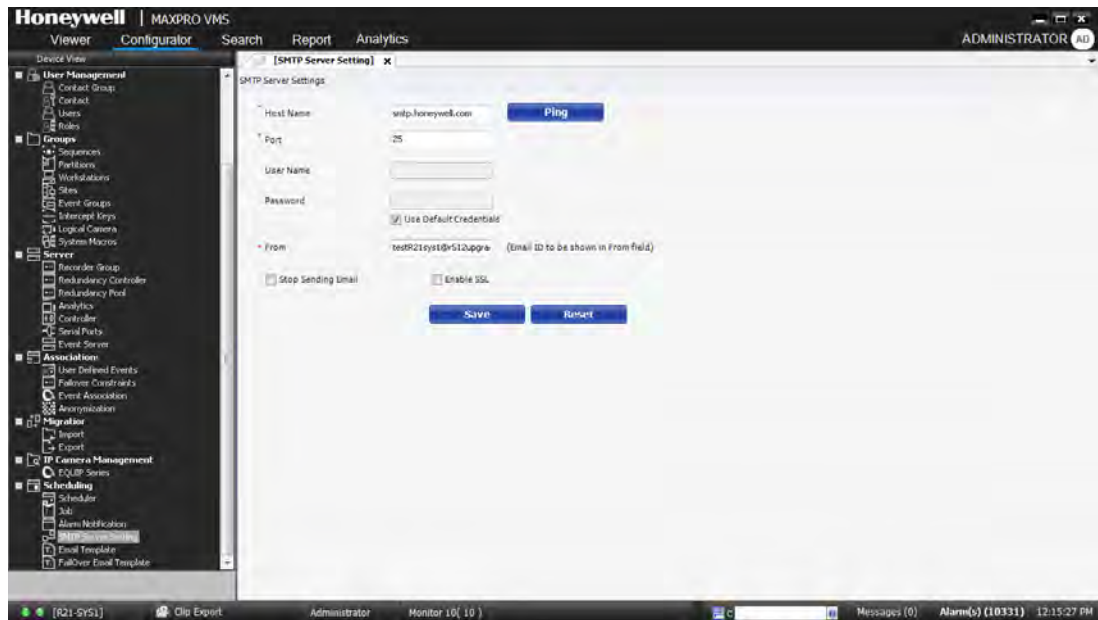


Figure 4-92 SMTP Server Settings

3. In the Host Name box, type a host name. Click Ping to verify the connection. The field appears in green if the IP address or the host name is valid.
4. In the Port Number box, the port number displays by default.
5. In the User Name box, type a name for the user.
6. In the Password text box, type a password for the user.

Note: Select the Use Default Credentials check box, if you want to use the credentials that were used while logging on. Honeywell recommends you to change the default Password before you logon to MAXPRO VMS. Refer to Securing MAXPRO VMS R550 Technical Notes for further details

7. In the From box, type the email address that should appear when an email is sent.

Note: Select Stop Sending Email, if you do not want to send an email from the configured settings.

8. Select the Enable SSL check box to enable the SSL settings.
9. Click Save.

Creating an Email Template

You can create an email template in MAXPRO VMS and use it while sending email notification about alarms to users.

To configure email template

1. Click the Configurator tab.
2. Expand Scheduling in the navigation area, and then click Email Template. The Email Template screen appears in the display area.

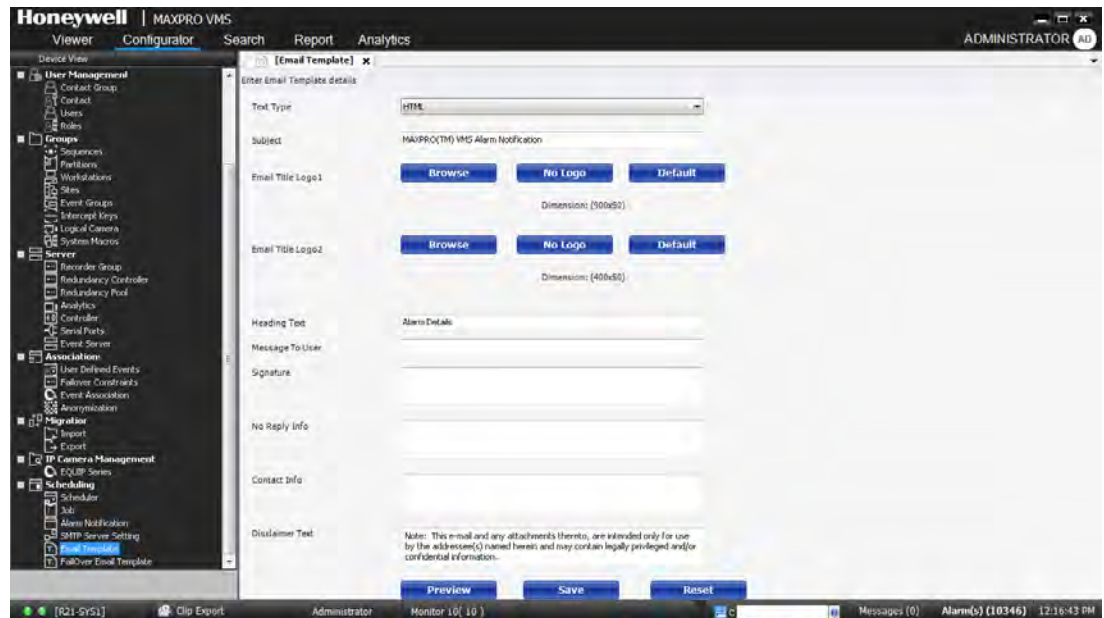


Figure 4-93 Email Template

3. From the Text Type drop-down list, select required text type for sending an email. The default text type is “HTML”.
4. In the Subject box, the default subject that appears in an e-mail displays. You can type a new subject as per your requirement.
5. In the Email Title Logo1 and Email Title Logo2, do one of the following:
 - a. Click Browse to browse and select the title logo image for the e-mail.
 - b. Click Default to retain the default logo image.
 - c. Click No Logo to remove the selected or default logo image.

Note: The dimension for Email Logo 1 should be 900 X 50 and for Email logo 2 should be 400 X 50.

4. In the Heading Text box, the default heading text displays. You can type a new heading text as per your requirement.
5. In the Message to User box, type the required message to user if any.
6. In the Signature box, provide the signature.
7. In the No Reply Info box, type the no reply message to the user if any.
8. In the Contact Info box, type the contact details for user to communicate.
9. In the Disclaimer Text box, the default disclaimer text displays. You can type a new disclaimer text as per your requirement.

10. Click Preview if you want to preview the e-mail.

Note: Click Reset, if you want to reset the email template.

11. Click Save.

Creating Failover Email Template

You can create an Failover email template in MAXPRO VMS and use it while sending email notification about failover to users.

To configure Failover email template

1. Click the Configurator tab.
2. Expand Scheduling in the navigation area, and then click Failover Email Template. The Failover Email Template screen appears in the display area.

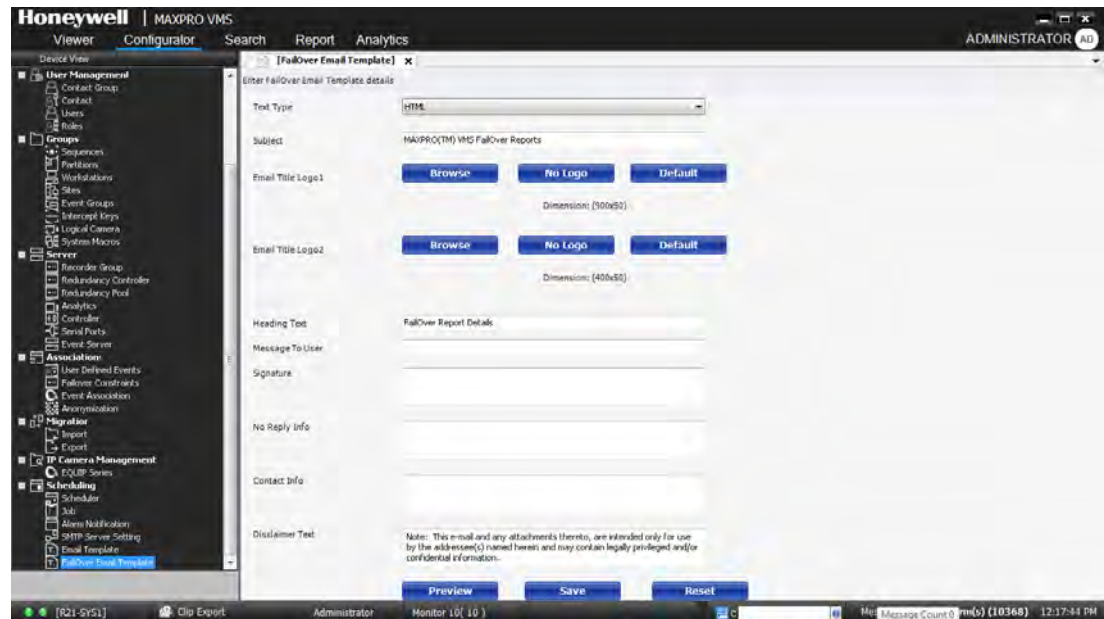


Figure 4-94 Failover Email Template

3. From the Text Type drop-down list, select required text type for sending an email. The default text type is “HTML”.
4. In the Subject box, the default subject that appears in an e-mail displays. You can type a new subject as per your requirement.
5. In the Email Title Logo1 and Email Title Logo2, do one of the following:
 - a. Click Browse to browse and select the title logo image for the e-mail.
 - b. Click Default to retain the default logo image.

- c. Click No Logo to remove the selected or default logo image.

Note: *The dimension for Email Logo 1 should be 900 X 50 and for Email logo 2 should be 400 X 50.*

4. In the Heading Text box, the default heading text displays. You can type a new heading text as per your requirement.
5. In the Message to User box, type the required message to user if any.
6. In the Signature box, provide the signature.
7. In the No Reply Info box, type the no reply message to the user if any.
8. In the Contact Info box, type the contact details for user to communicate.
9. In the Disclaimer Text box, the default disclaimer text displays. You can type a new disclaimer text as per your requirement.
10. Click Preview if you want to preview the e-mail.

Note: *Click Reset, if you want to reset the Failover email template.*

11. Click Save.

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](#) on page 322.

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.

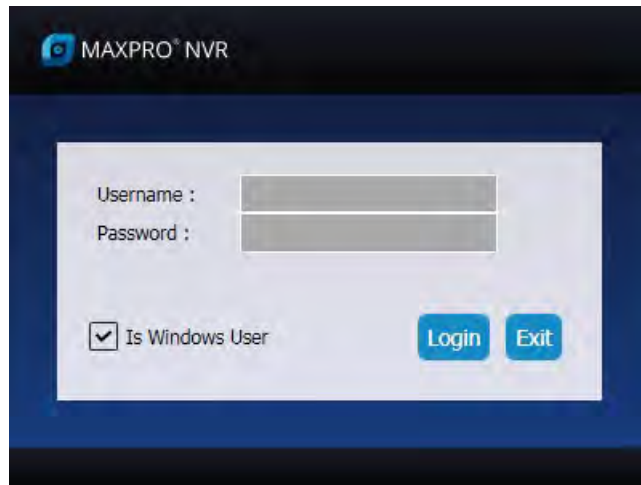


Figure 4-95 Meta Data Conversion Utility Login

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 as shown below.

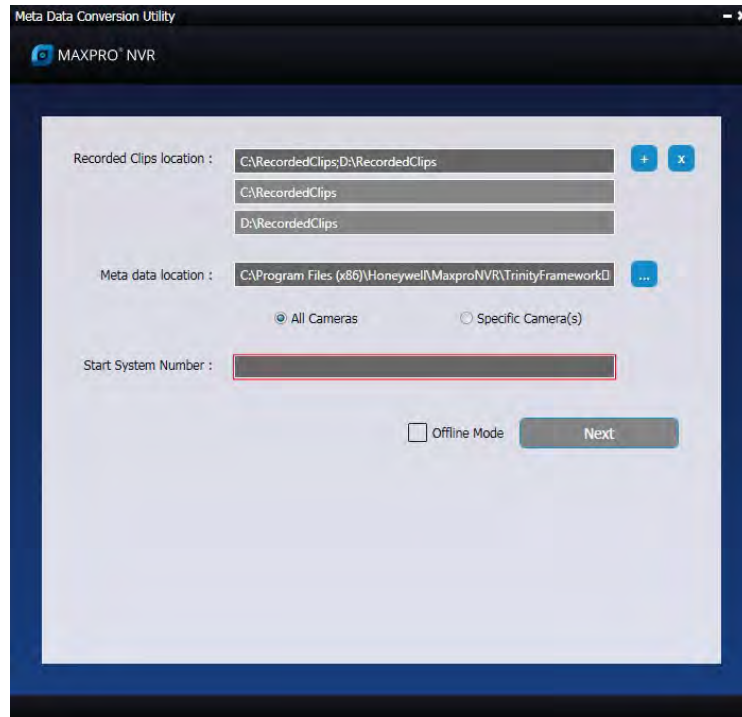





Figure 4-96 Meta Data Conversion Utility

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](#) on page 319. 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  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.

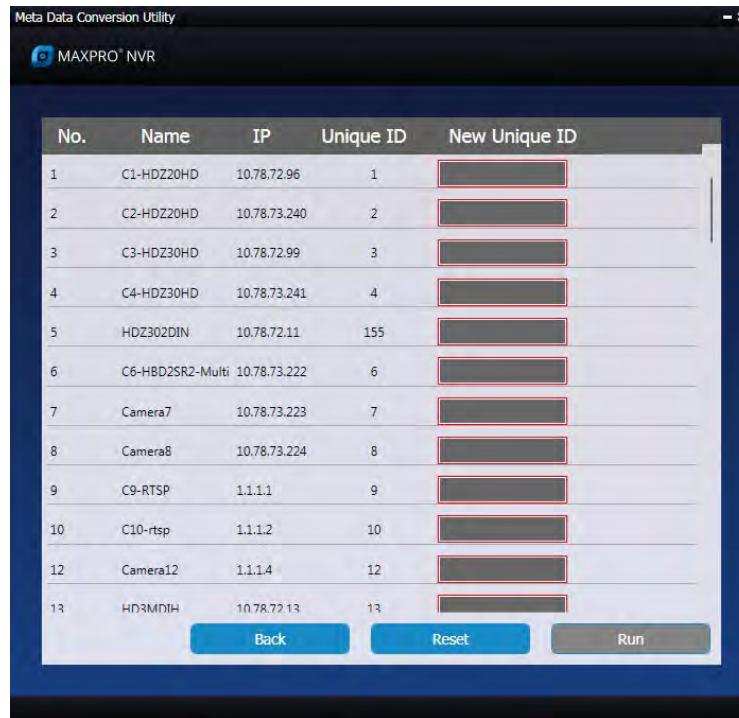


Figure 4-97 Define Unique ID screen

7. Click Run to execute the utility.
Or
Click Back to go 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](#) on page 320.
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.



Figure 4-98 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.

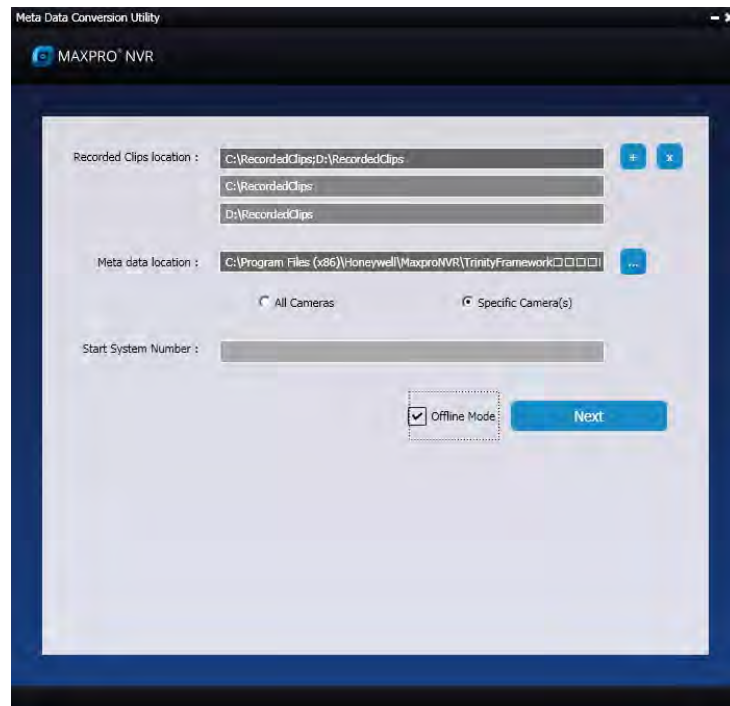


Figure 4-99 Offline Mode

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.

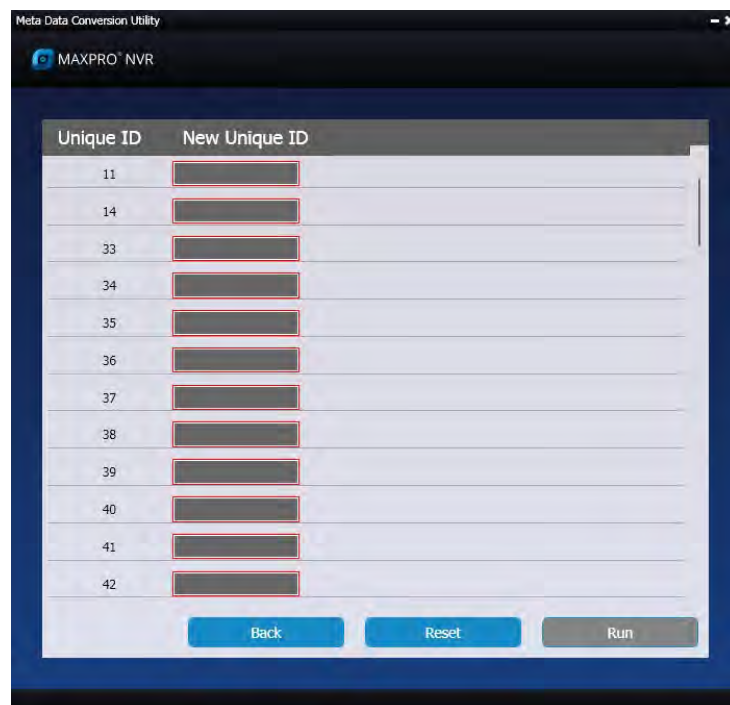


Figure 4-100 Offline Updating Unique ID

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.

Video Analytics Events

The following table displays the 5 default Video Analytics Events with description and severity level supported in MAXPRO VMS R600. New EquiP series model cameras (HFD6GR1, HSW2G1, HCD8G, HBD8GR1, H4D8GR1, HDZ302DE, HDZ302D, HDZ302DIN) generates the following events in NVR box.

Note: User need to configure the following events in the camera web page to view in the Alarms window.

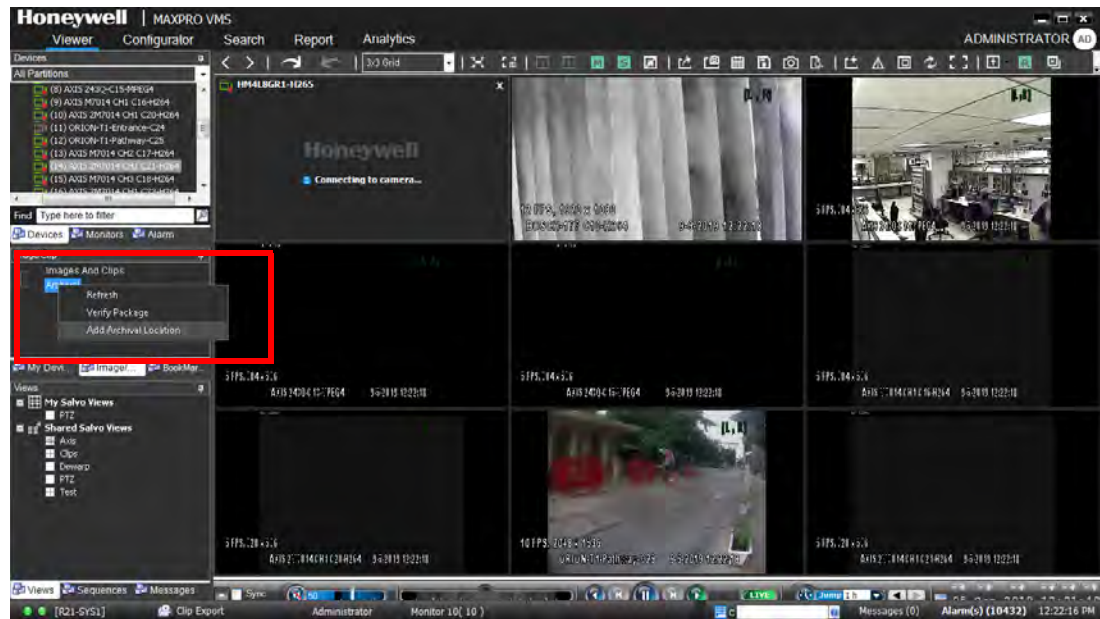
EventID	EventDescription	EventSeverity
2066	Face Detected	40
	Tamper Detected	
	Audio Detected	
	Device SD Card Full	
	Device SD Card Failure	

Manual Archival For Recorders

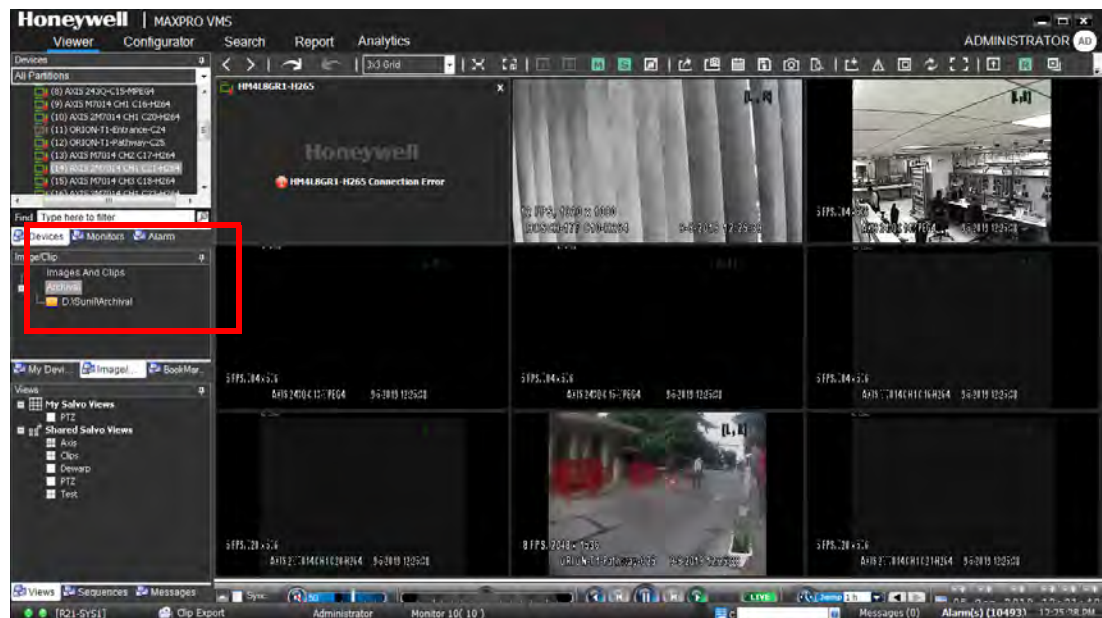
To manually archive primary and redundant recorders:

Note: Before performing the manual archive ensure that you configure the Drive path in NVR.

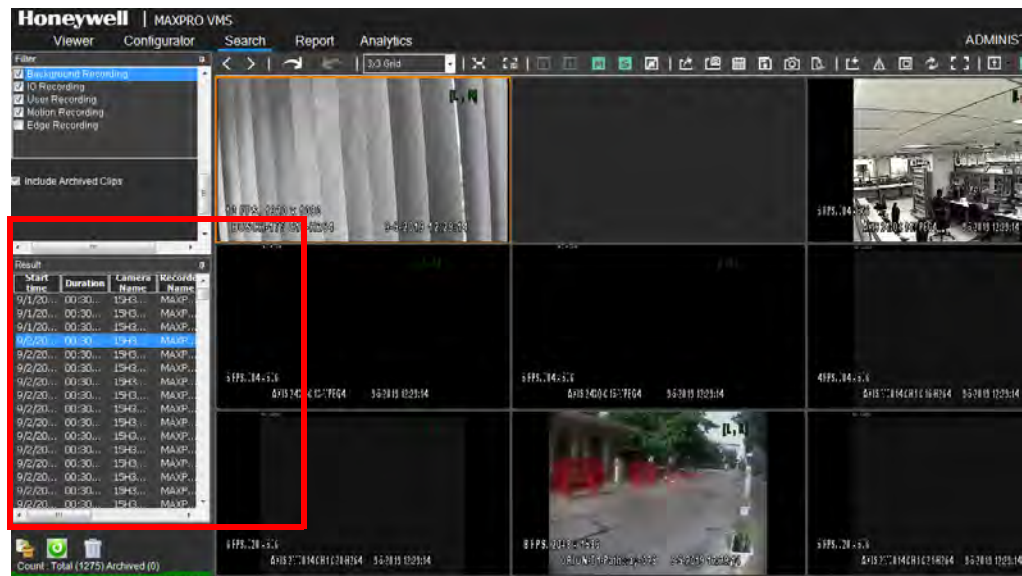
1. In Viewer, navigate to Images and Clips > Default > Archival and then map the drive location which you have created in NVR as shown below.




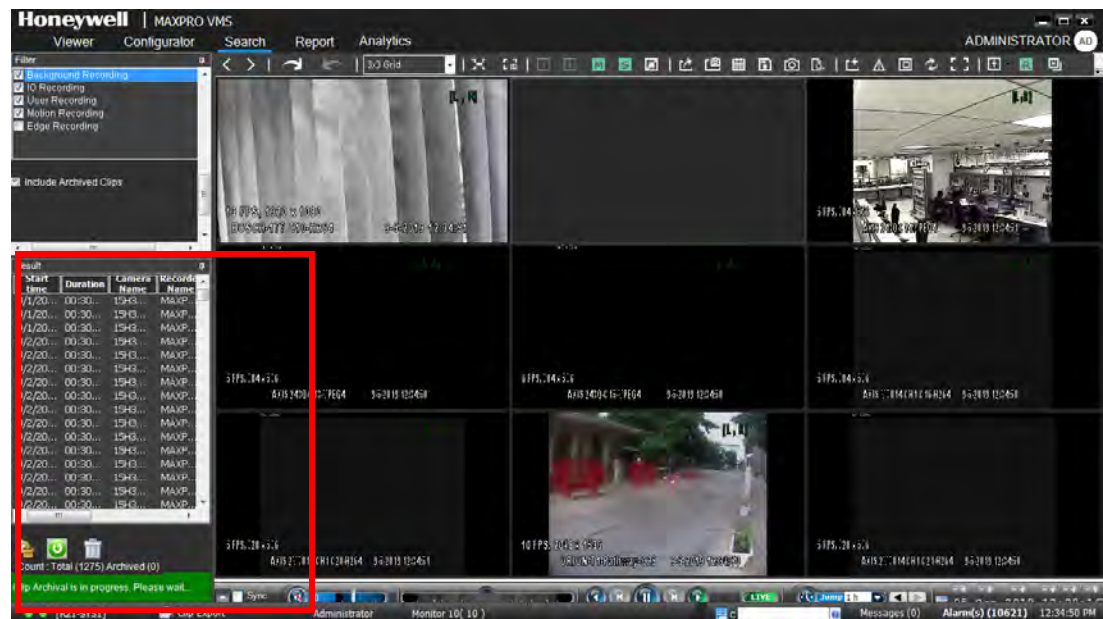
2. Right-click on Archival > Add Archival location, the Browse for Folder page appears.
3. Under Network drive, select the NVR recorder machine name
4. Map the storage path of the Recorder Machine IP under which you want to save the recordings. Provide the recorder Machine IP details of the path in VMS as shown below.



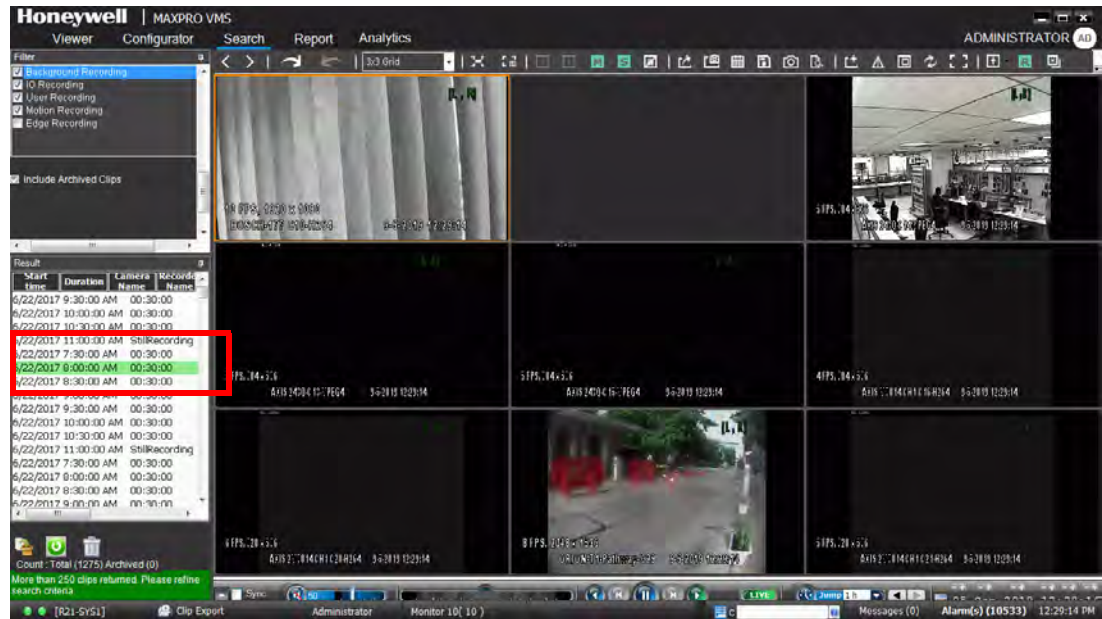
5. In the Search tab, search for the Clips. Refer to [MAXPRO® VMS Operators Guide](#) for more information on how to search recorded videos/clips. The list of recordings of both primary and redundant recorders are displayed as shown below.



6. Select the required recordings/clips from the list and then click . The clip Archival Progress is displayed at the bottom as shown below.



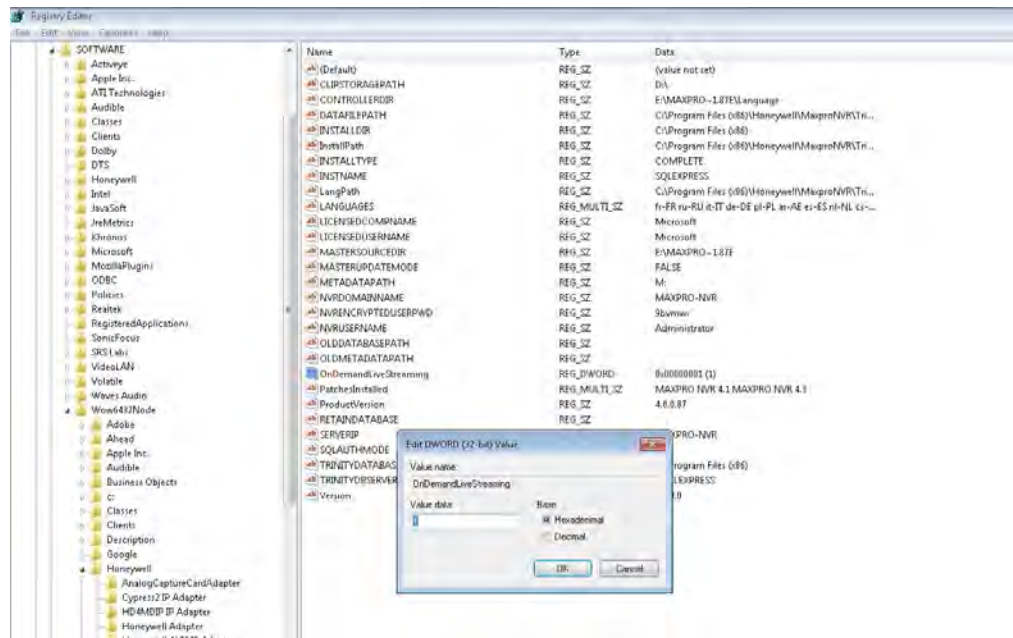
Once the Archival is success the selected clip turn to **Green** as highlighted below. If the Archival fails then the selected clip is displayed in **Red**. The archived clip is saved under configured machine and drive path.



Enabling Video on demand feature

To enable video on demand feature in MAXPRO NVR:

1. Navigate to the below registry path HKEY_LOCAL_MACHINE->SOFTWARE->Wow6432Node->Honeywell->MaxproNVR->TrinityFramework->OnDemandLiveStreaming
2. 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.



3. Restart both the NEO (NEO 1 and 2) services.

Note: In VMS, no need to perform any settings or configuration changes to enable VOD feature. No recordings will take place in NVR once Video On Demand feature is enabled.

How to Enable/Disable Cameras and Stream

To Enable/Disable the cameras or camera stream and redirect to NVR in ISOM perform the following:

1. Navigate the path in NVR C:\Program Files (x86)\Honeywell\UVISOM.

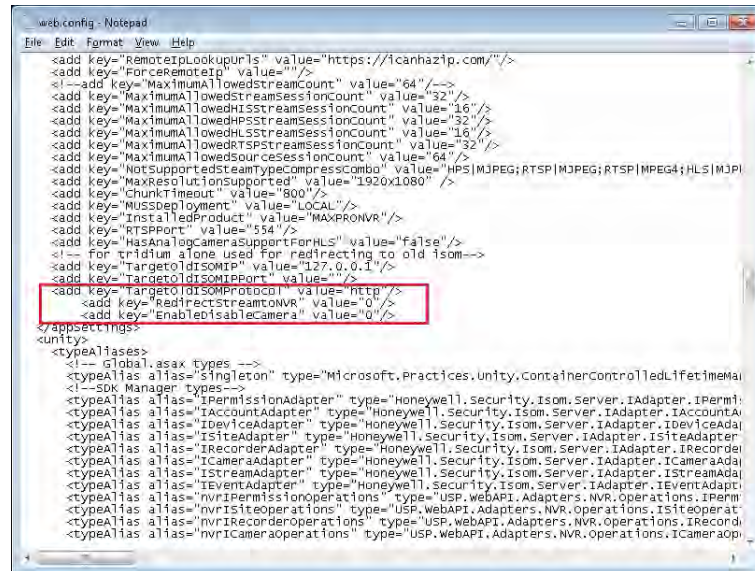
2. Open web.config file in notepad and check the below 2 entries:

```
<add key="RedirectStreamtoNVR" value="0"/>
```

```
<add key="EnableDisableCamera" value="0"/>
```

3. By default both are set to "0". (disabled). To enable the feature, change the value from 0 to 1 as highlighted below.

Note: Once Video On Demand is configured in MAXPRO NVR then Enable/Disable camera feature can be turned off.



```
web.config - Notepad
File Edit Format View Help

<add key="RemoteIpLookupUrl" value="https://icanhazip.com/" />
<add key="ForceRemoteIp" value="" />
<!--add key="MaximumAllowedStreamCount" value="64" /-->
<add key="MaximumAllowedStreamSessionCount" value="32" />
<add key="MaximumAllowedHLSStreamSessionCount" value="16" />
<add key="MaximumAllowedHPSStreamSessionCount" value="32" />
<add key="MaximumAllowedRTSPStreamSessionCount" value="32" />
<add key="MaximumAllowedSourceSessionCount" value="64" />
<add key="NotSupportedStreamTypecompressCombo" value="HPS|MJPEG;RTSP|MPEG4;HLS|MJPEG" />
<add key="MaxResolutionSupported" value="1920x1080" />
<add key="ChunkTimeout" value="800" />
<add key="MUSDeployment" value="LOCAL" />
<add key="InstalledProduct" value="MAXPRONVR" />
<add key="RTSPPort" value="554" />
<add key="HasAnalogCameraSupportForHLS" value="false" />
<!-- for triduum alone used for redirecting to old isom-->
<add key="TargetOldISOMIP" value="127.0.0.1" />
<add key="TargetOldISOMIPPort" value="" />
<add key="TargetOldISOMIPProtocol" value="http" />
<add key="RedirectStreamONVR" value="0" />
<add key="EnableDisableCamera" value="0" />
</appSettings>
<unity>
  <typeAliases>
    <!-- Global.asax types -->
    <typeAlias alias="singleton" type="Microsoft.Practices.Unity.ContainerControlledLifetimeManager" />
    <!-- SDK Manager types -->
    <typeAlias alias="IPermissionAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IPermissionAdapter" />
    <typeAlias alias="IAccountAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IAccountAdapter" />
    <typeAlias alias="IDeviceAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IDeviceAdapter" />
    <typeAlias alias="ISiteAdapter" type="Honeywell.Security.Isom.Server.IAdapter.ISiteAdapter" />
    <typeAlias alias="IRecorderAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IRecorderAdapter" />
    <typeAlias alias="ICameraAdapter" type="Honeywell.Security.Isom.Server.IAdapter.ICameraAdapter" />
    <typeAlias alias="IStreamAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IStreamAdapter" />
    <typeAlias alias="IEventAdapter" type="Honeywell.Security.Isom.Server.IAdapter.IEventAdapter" />
    <typeAlias alias="nvrIPermissionOperations" type="USP.WebAPI.Adapters.NVR.Operations.IPermissionOperations" />
    <typeAlias alias="nvrISiteOperations" type="USP.WebAPI.Adapters.NVR.Operations.ISiteOperations" />
    <typeAlias alias="nvrIRecorderOperations" type="USP.WebAPI.Adapters.NVR.Operations.IRecorderOperations" />
    <typeAlias alias="nvrICameraOperations" type="USP.WebAPI.Adapters.NVR.Operations.ICameraOperations" />
  </typeAliases>
</unity>
```

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 Enable/Disable Cameras and Stream](#) section.

Note: Make sure MAXPRO Web client is working.

How to Configure Profile-G or Edge Sync Feature

To configure the Profile-G or Edge Sync feature, perform the following in the order mentioned:

1. Upgrade the Camera Firmware.
 - Enable SD card recording with required settings
1. Upgrade MAXPRO NVR to the latest version
2. Configure the Edge Sync Settings
 - Enable the Edge Sync feature

Upgrade the Camera

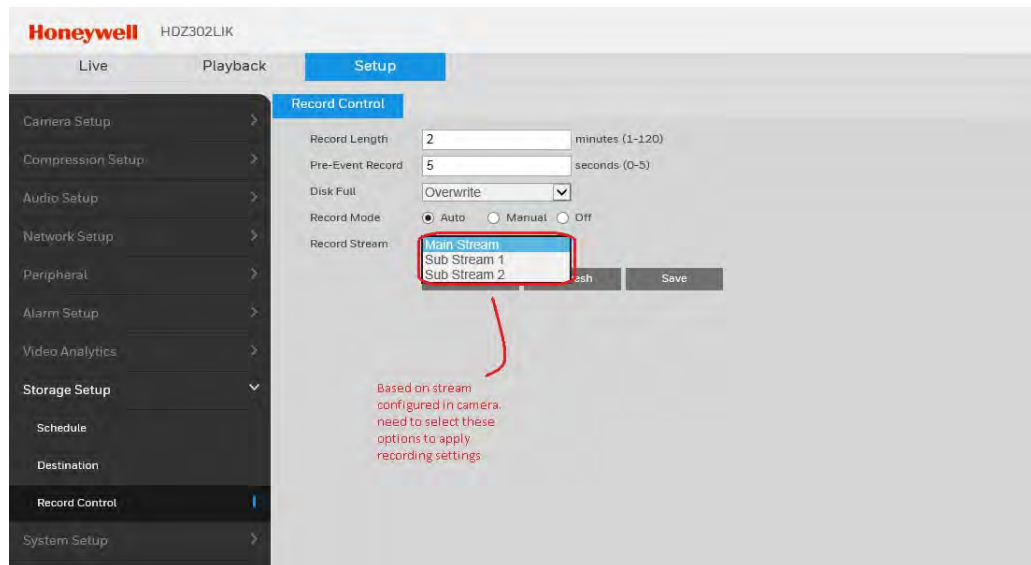
Before Upgrading

- If there are critical recordings available in SD card, please take back up using camera web page before upgrading the firmware.
- Upgrade to the Camera Firmware versions to latest versions as mentioned in the above table.
- It is recommended to use IPC utility to upgrade the Camera Firmware.

Note: *Ensure that there is no Camera power fluctuations during the upgrade procedure. This is to ensure smooth camera firmware upgrade.*

Post Upgrade (Camera Settings)

1. Before adding the Profile-G camera into NVR, delete all the existing recording available in SD card.
2. Configure the required SD card recording configuration in the camera Webpage



Note: Irrespective of the length/size of clips, maximum number of clips supported on SD card is 700 only.

If user want to use secondary channels resolution for SD card recording they have to set SD card recording settings as per the stream selected.

3. Ensure that the Camera Timezone is adjusted to match with the MAXPRO NVR machines time zone.
4. Select the Synchronize with check box to sync the NTP time server with Camera time and MAXPRO NVR time.

Upgrade MAXPRO NVR

- Install the MAXPRO NVR 4.5 Build 162 on top of NVR 4.1 Build 123. Refer [MAXPRO® NVR Installation and Configuration Guide](#) for more information on how to upgrade.

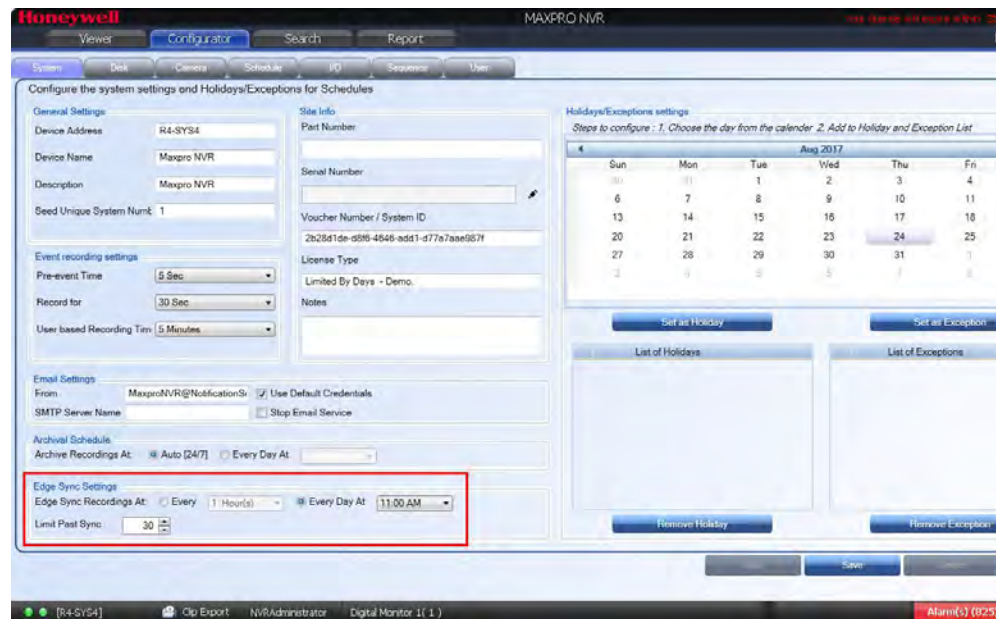
Configure the Edge Sync Settings

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.

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.

To configure the Edge Sync Settings:

1. In MAXPRO NVR, navigate to Configurator > Systems tab. The Systems screen is displayed as shown below.



2. Under Edge Sync Settings:
 - Click Every option and then select the time in minutes or hours to edge sync the recordings.
Or
Click Every Day at option and then select the specific time in hours during which the edge sync 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.

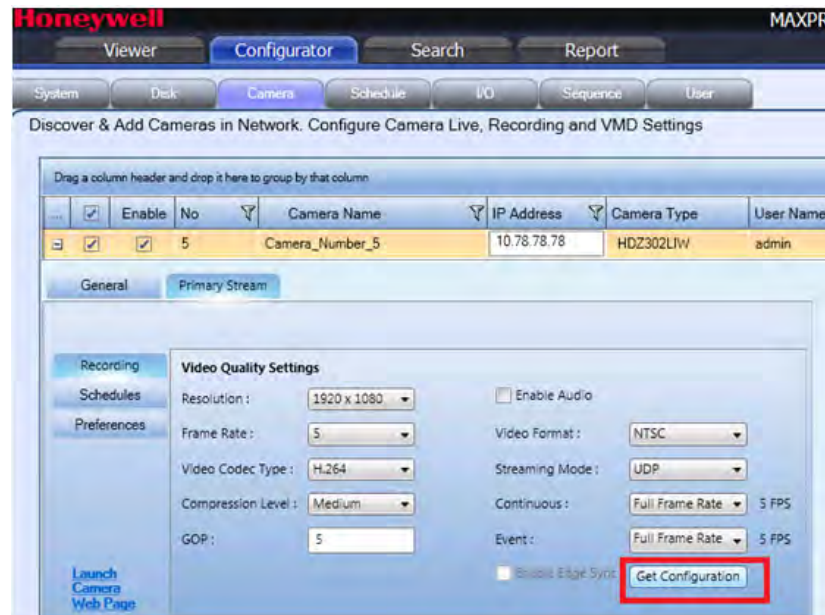
Note: The default Archival Schedule configured and recommended is Every Day at 12:00 AM. This is recommended versus the Auto [24/7] option for optimal performance and load on NVR.

Enable the 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.

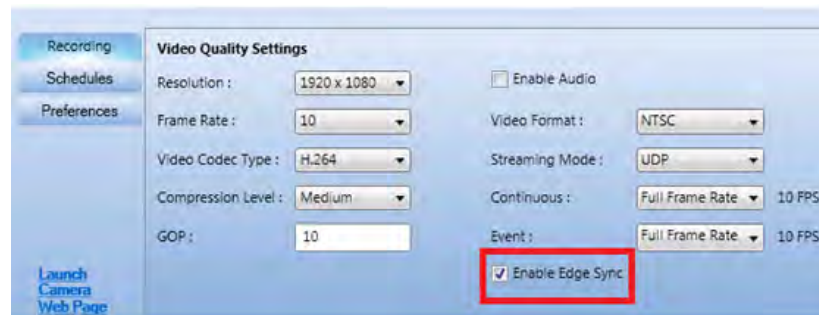
To enable the Edge sync option:

1. Navigate to Configurator > Camera tab. The Camera screen is displayed as shown below.

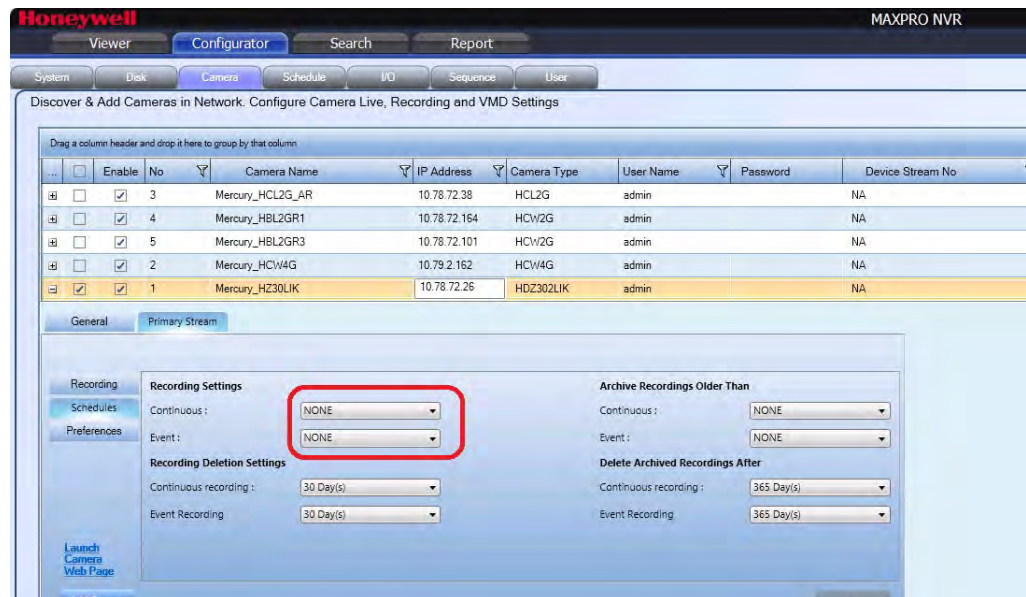


2. Click the Get Configuration button. If the camera is a Profile-G compliant camera then the Get Configuration button disappears and Enable Edge Sync check box is enabled as shown below.
If the camera is not Profile-G compliant then NVR application displays Edge Sync not supported or enabled for this device message at the bottom of the screen.

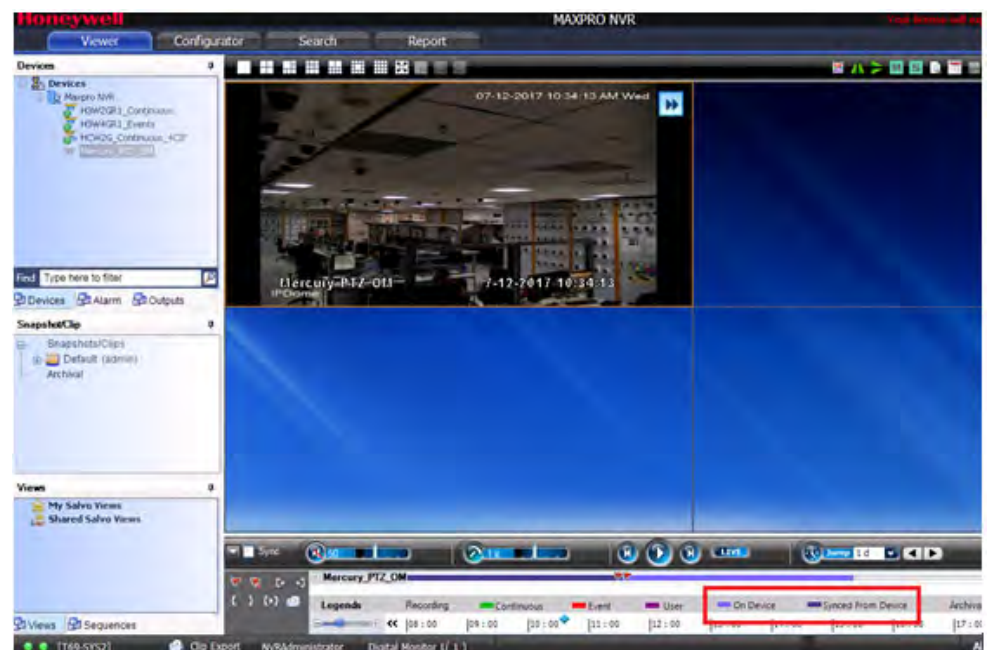
Note: For Profile-G compliant cameras the Streaming Mode is defaulted to UDP. If you want to switch from UDP to TCP mode then you need to update the .config file. After modifying the .config file for TCP mode you need to restart the Trinitybackfill service.



3. Select the Enable Edge Sync check box and then click Save.
4. Under Schedule tab > Recording Settings, select None from the drop-down list for both Continuous and Event based recording for the camera as shown below.



Once the Edge syncing is enabled you can see the recordings available in SD card and in MAXPRO NVR (after Edge syncing) as highlighted below:

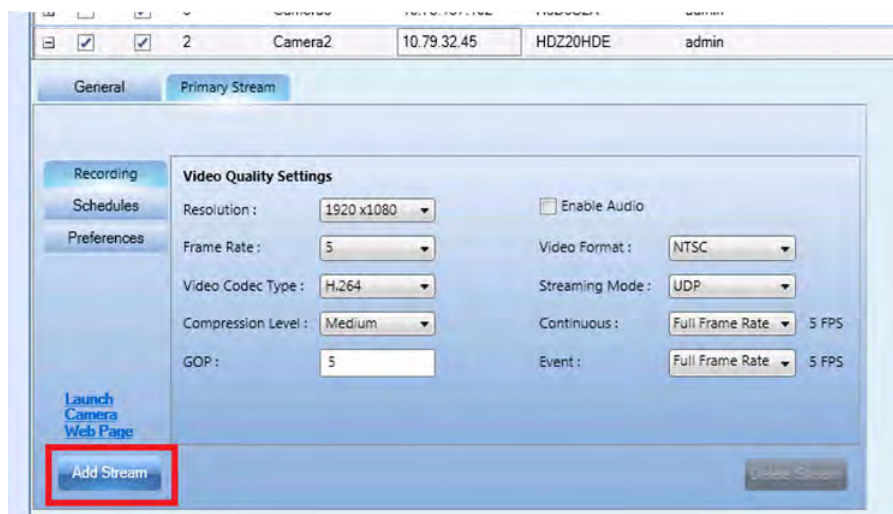


Note: You can Playback only the Edge synced clips (synced clips from camera SD card to MAXPRO NVR) from the MAXPRO NVR clients.

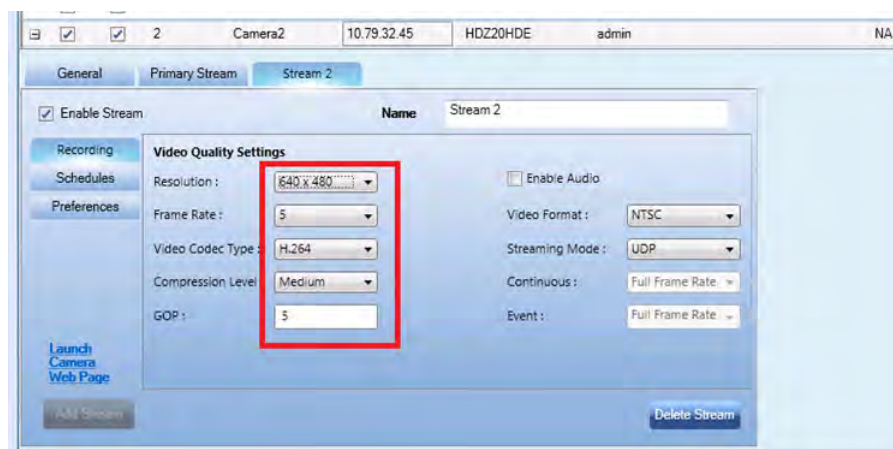
How to Enable Low Bandwidth Streaming

To enable Low Bandwidth Streaming from MAXPRO NVR cameras to MAXPRO VMS clients:

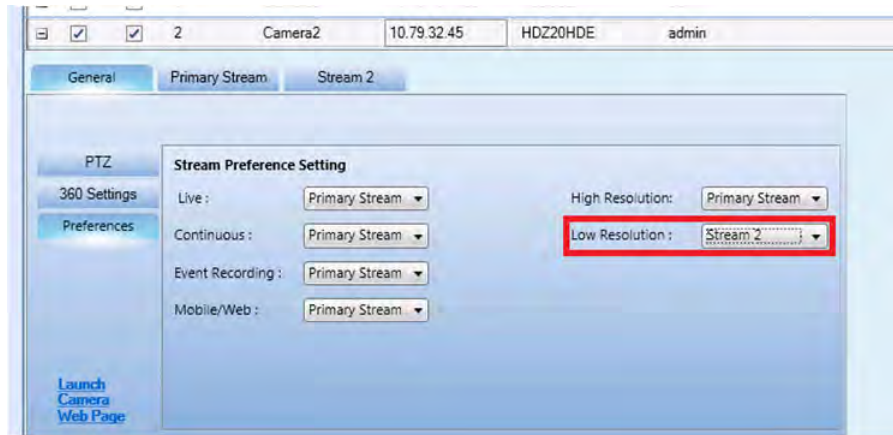
1. In MAXPRO NVR > Configurator> Camera > Primary Stream tab, click Add Stream to add a secondary stream for the camera as highlighted below. A new stream (Stream 2) is added.



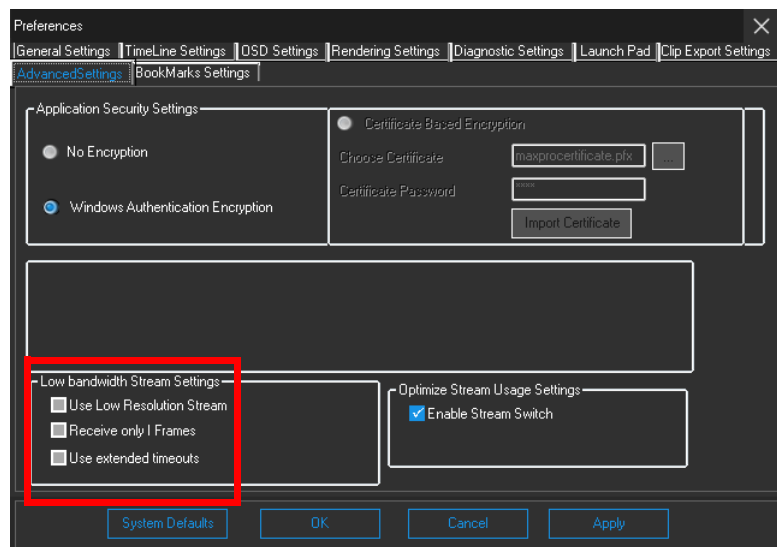
2. Under Stream2 > Recording > Video Quality Setting, select the low Resolution, FPS and GOP from the corresponding drop-down lists as highlighted below.



3. Under General tab > Preferences > Stream Preference Settings, select Stream 2 from the Low Resolution drop-down list to set the Low Resolution configuration to use Secondary stream as shown below.



4. Once you are done with the configuration in NVR, discover the same MAXPRO NVR recorder in the MAXPRO VMS Server.
5. In MAXPRO VMS Client, click the Preferences Tab and navigate to the Advanced settings tab. This tab allows you can configure to use necessary setting applicable for this client as highlighted below.

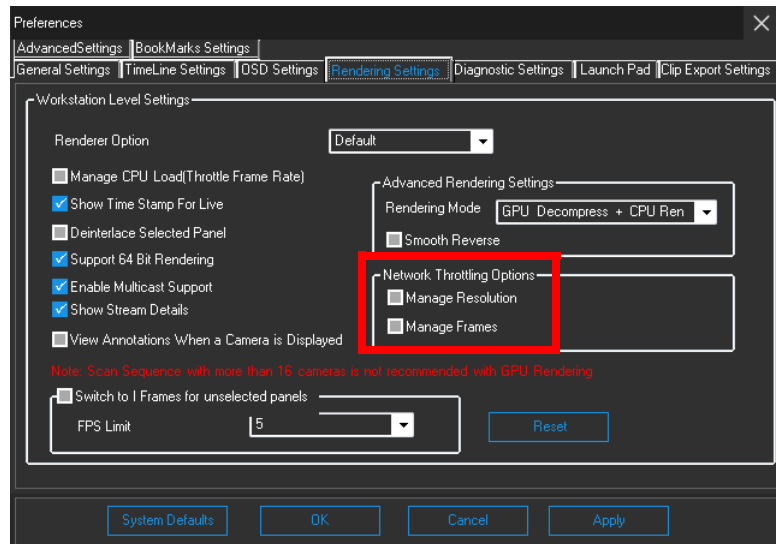


6. Under Low bandwidth Stream Settings:
 - Select Low Resolution Stream check box - To enable and use only low resolution stream from MAXPRO NVR.
 - Select Receive only I Frames check box - It allows you to receive only I frames for the camera stream. (For example: If a Camera is configured with 5 FPS and 5 GOP and if you select this check box then this setting will pull only I frame for the camera stream. It excludes P frames for the camera stream. This setting can be used when the available bandwidth is too low for full frames rendering of Secondary streams.)

- Select the Use Extended Timeouts check box – This helps in increasing the default time outs for NVR connections, stream connections and snapshots retrieval.

Note: The above highlighted options will be disabled if you select Network Throttling Options (Manage Resolutions & Manage FPS) in Rendering Settings tab.

7. Click the Rendering settings tab. This tab allows you can configure to the Network Throttling options for low bandwidth site.
 8. Under Network Throttling Options: This feature automatically measures the latency in streams periodically and manages the stream with lower resolution and lower frame rate in low network bandwidth sites. This enables user to view smooth video without fluctuations.
- Manage Resolution: Select this check box to manage the fluctuations in the resolutions.
 - Manage Frame: Select this check box to manage the frames per second in a video.



Note: These settings can be enabled and used in Winmag machines where VMS clients are installed. After using these setting low streams can be pulled from Winmag viewer as well.

Enhancing Live Video Streaming in Low Bandwidth Site

Depending on the available network bandwidth at Site, for better user experience and to enhance the performance of Live video streaming, user needs to manually configure the config file and the Registry entries.

How to configure the Registry entries For "NetworkMonitorPeriod"

1. Navigate to:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Honeywell\TrinityFramework\RenderingServer (for 32 bit machines)
Or
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Honeywell\TrinityFramework\RenderingServer (for 64 bit machines)
2. Open with Notepad and locate "NetworkThrottleBackPeriod" parameter. See the table below for description and change the value accordingly.

Entry to configure	Default Value	Description
NetworkThrottleBackPeriod	300000 Milli Seconds	This value is in Milli Seconds. This is a waiting period during which if no latency is detected on a stream, an attempt will be made to increase the stream parameters. For a good network this can be set at a lower value and for a network where the network disturbances are high or bandwidth availability is low it can be set to a high value.

3. Save the file once done.
For NetworkMonitorPeriod

1. Navigate to:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Honeywell\REAdapter (for 32 bit machines)
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Honeywell\REAdapter (for 64 bit machines)
2. Open with Notepad and locate "NetworkMonitorPeriod" parameter. See the table below for description and change the value accordingly.

Entry to configure	Default Value	Description
NetworkMonitorPeriod	5000 Milli Seconds	It is internal polling interval to monitor latency in packets delivery. This registry value should not be changed.

3. Save the file once done.

For SystemLevelStreamCompensation

1. Navigate to:
 - HKEY_LOCAL_MACHINE\SOFTWARE\Honeywell\TrinityFramework\RenderingServer (32 bit machines)
 - HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Honeywell\TrinityFramework\RenderingServer (64 bit machines)

2. Open with Notepad and locate “SystemLevelStreamCompensation” parameter. See the table below for description and change the value accordingly.

Entry to configure	Default Value	Description
SystemLevelStreamCompensation	1	If this is enabled (1) then load balancing will be done on streams from same NVR to this VMS client. This registry value should not be changed.

3. Save the file once done.

How to configure the Config File entries

1. Navigate to C:\Program Files\Honeywell\TrinityFramework\Bin\
2. Locate MMShell.exe.Config and open with Notepad. See the table below for description and change the value accordingly.

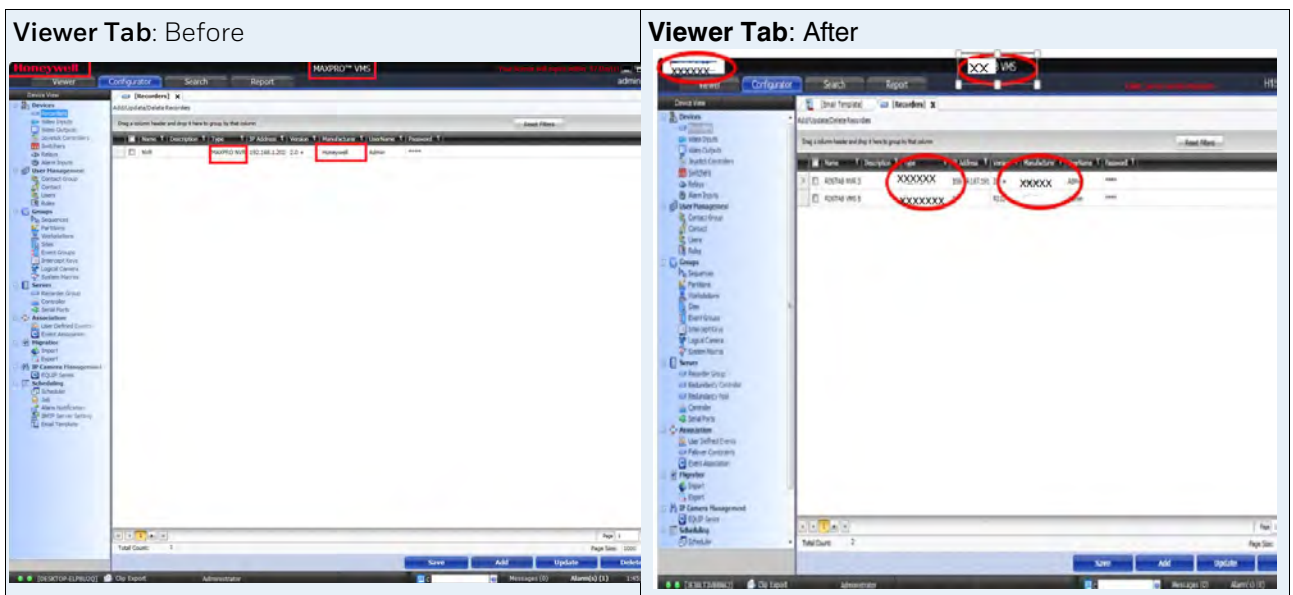
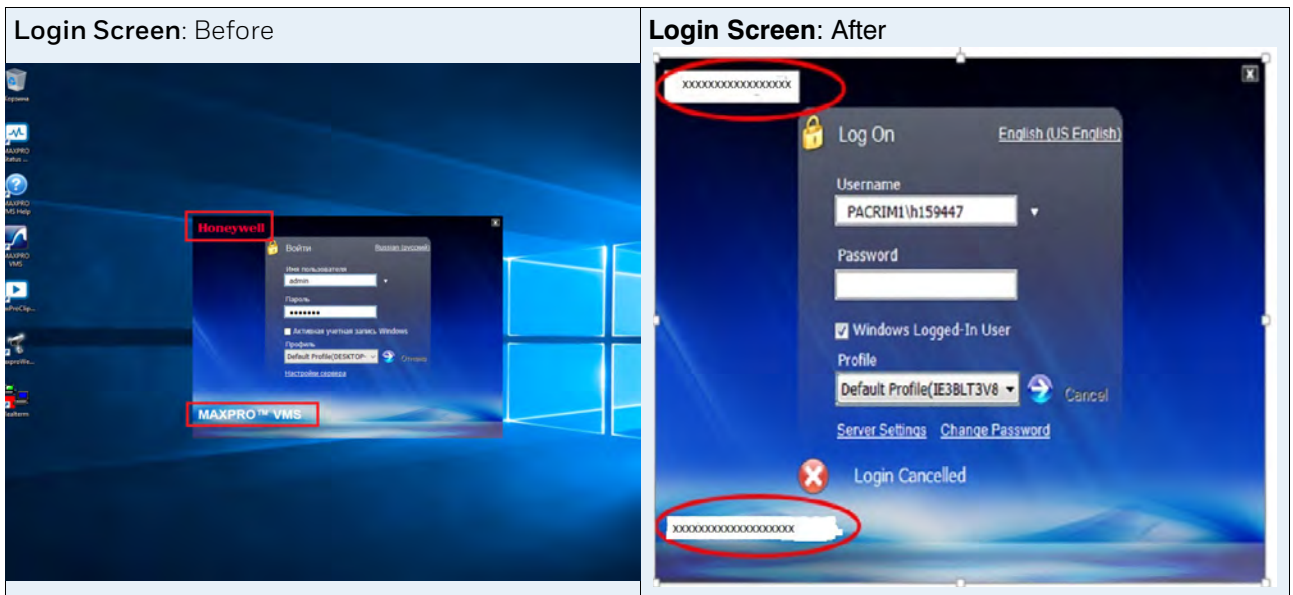
Entry to configure	Default Value	Description
<add key="NetworkThrottlingThresh oldTime" value="1000" />	1000 Milli Seconds	The value is in Milli seconds. This is the allowed latency streams due to limited bandwidth. If a stream is experiencing latency by a value greater than this, then network throttling will try to reduce the stream parameter. This is a tuning parameter and 1000 should hold good for general scenarios. Based on site network conditions this can be varied.

3. Save the file once done.

Custom Branding Utility

Custom Branding Utility enables a business organization to customize the brand parameters based on their requirement. This utility provides the flexibility to customize the company brand name, logo, Watermark, Product logo and Product name.

Below sample images illustrates the before and after screens with customized brand name and logo.



How to access the Utility

User can contact to Honeywell Dealer or Tech support to obtain this utility. Please see the back cover for contact information.

How to Customize the Brand

To customize the brand parameters:

Note: Before running the customization utility ensure that you close the MMShell and MAXPRO VMS Client Agent applications. This utility should be executed separately on both Server and client to customize the brand parameters.

1. Double-click the CustomizationUtility.exe available on your desktop. The Custom branding Utility screen is displayed as shown below.

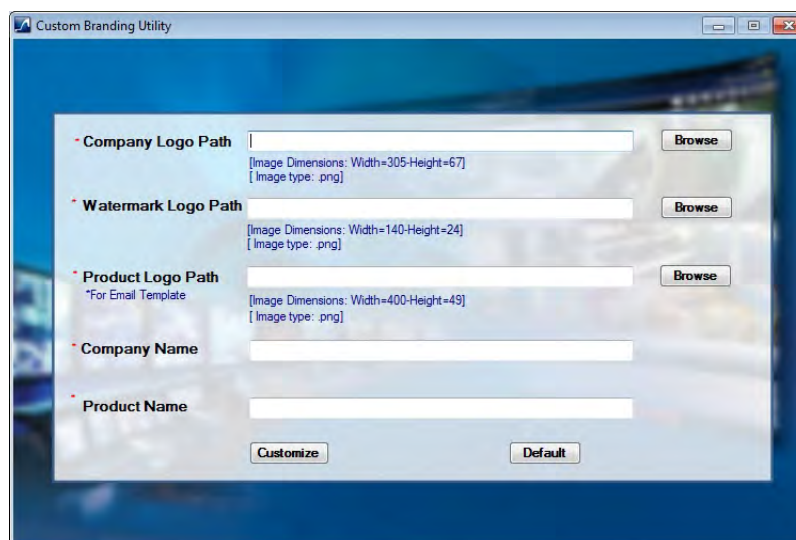


Figure 4-101 Custom Branding Utility

2. Click the Browse button to choose and upload the following details:
 - Company Logo Path. The Image Dimensions should be Width: 305 and Height: 67. The supported image format is .png file format.
 - Watermark Logo Path. The Image Dimensions should be Width: 140 and Height: 24. The supported image format is .png file format.
 - Product Logo Path: This is specific to Email Template. The Image Dimensions should be Width: 400 and Height: 49. The supported image format is .png file format.
3. Type the required Company Name in the box provided. The maximum number of characters allowed is 20.
4. Type the required Product Name in the box provided. The maximum number of characters allowed is 25.
5. Click Customize to upload the details. A message Application has been customized successfully is displayed as shown below.

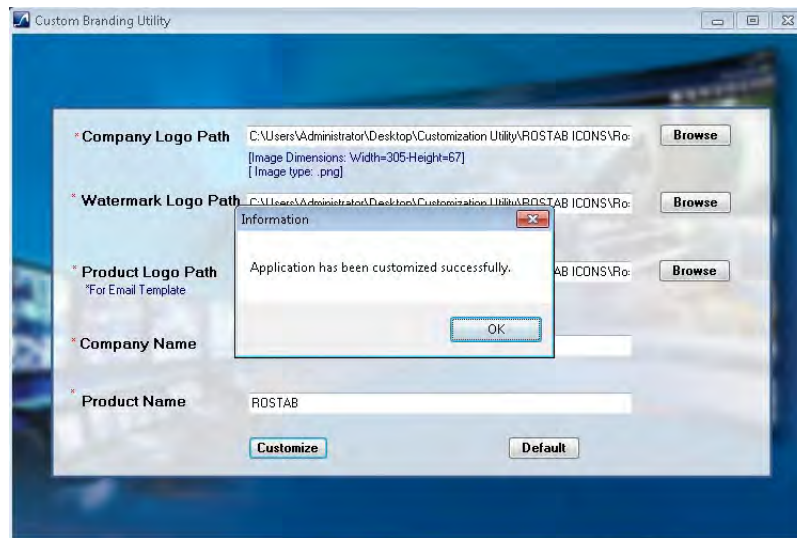


Figure 4-102 Custom Branding Success

Or
Click Default to reset the parameters back to MAXPRO VMS. A message Application has been reset to default settings is displayed as shown below.

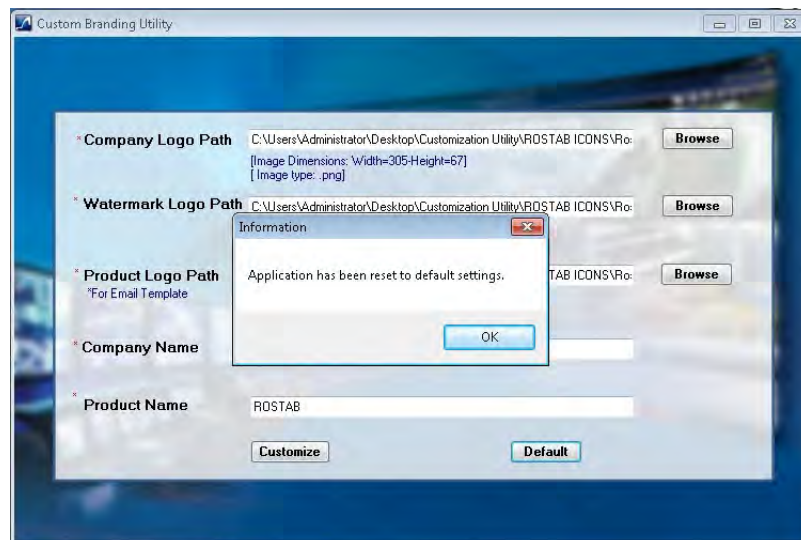


Figure 4-103 Custom Branding Default Success

Configuring Multicast

User needs to perform the following configurations in the order as explained below to view the Multicast stream:

1. Switch Configuration
2. Camera Configuration:
3. MAXPRO® NVR Configuration
4. MAXPRO® VMS Configuration

Step1 - Switch Configuration

- Enable IGMP Snooping Global Settings option in the Multicast section of the switch as highlighted below.

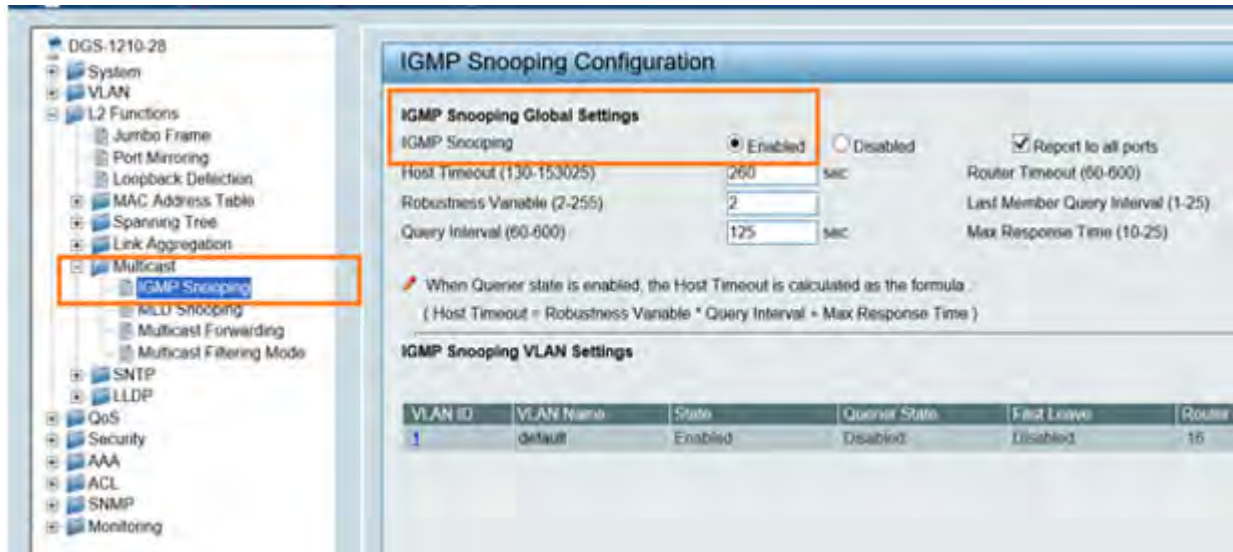


Figure 4-104 Switch Configuration

Step2 - Camera Configuration

1. In the camera web page navigate to Setup tab > Network Setup > Multicast screen, enable Multicast option as highlighted below.
2. Type the Multicast Address and Port details. The full range of Multicast addresses is from 224.0.0.0 to 239.255.255.255 and port numbers is from 1025 to 65529.

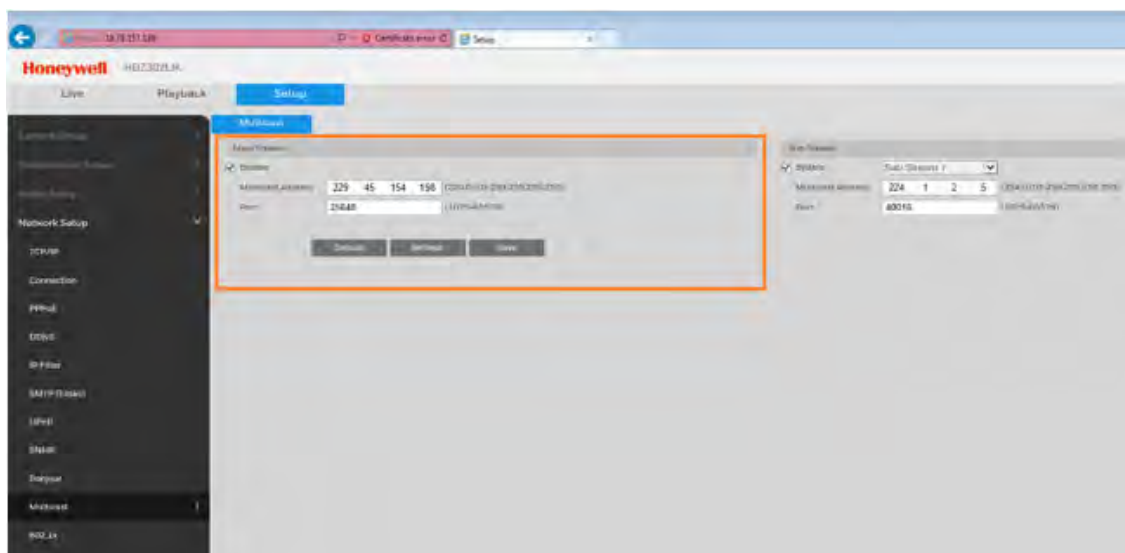


Figure 4-105 Camera Configuration

The following table lists the camera models supported for Multicast feature and corresponding Camera Type & Firmware details:

Equip -S Mercury Series Cameras	Camera Type	Firmware Details
H4W2GR1	Outdoor Dome 2MP 2.7-12mm	V1.000.HW00.6, build: 2017-10-16
H4W2GR2	Outdoor Dome 2MP 7-22mm	
H4W4GR1	Outdoor Dome 4MP 2.7-12mm	
H3W2GR1	Indoor Dome 2MP 2.7-12mm	
H3W2GR2	Indoor Dome 2MP 7-22mm	
H3W4GR1	Indoor Dome 4MP 2.7-12mm	
HBW2GR1	Bullet 2MP 2.7-12mm	
HBW2GR3	Bullet 2MP 4.7-47mm	
HBW4GR1	Bullet 4MP 2.7-12mm	
HCW2G	Box 2MP	
HCW4G	Box 4MP	

Equip -S Mercury Series Cameras	Camera Type	Firmware Details
HCL2G	Box 2MP low light	V2.420.HW01.19, build: 2017-10-16
H4L2GR1	Outdoor Dome 2MP 2.7-12mm low light	
HBL2GR1	Bullet 2MP 2.7-12mm low light	
HDZ302LIW	IR PTZ wiper, low light	Software Version: 1.000.0037.0, Build 2017-12-01 PTZ version: 1.000.000.20171128 Module version: 01.06.0A
HDZ302LIK	IR PTZ IK10, low light	

Step3 - Configuration in MAXPRO® NVR

1. For a specific camera, enable Multicast option in NVR Configurator > Camera properties page as highlighted below.
2. Type the Multicast Address and Port details accordingly.

Note: Only H.264 Codec format is supported to view Multicast Stream. Sub-streams are not supported.

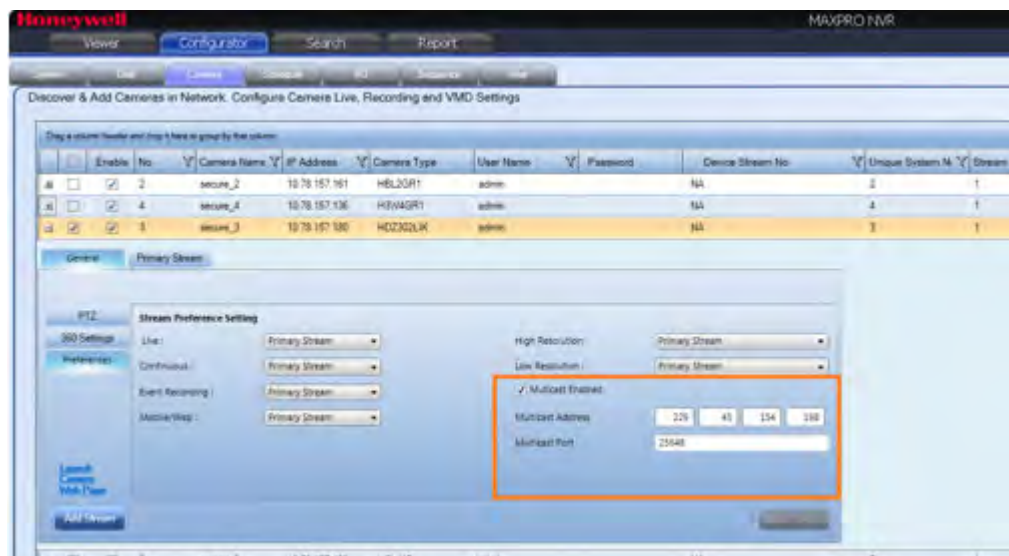
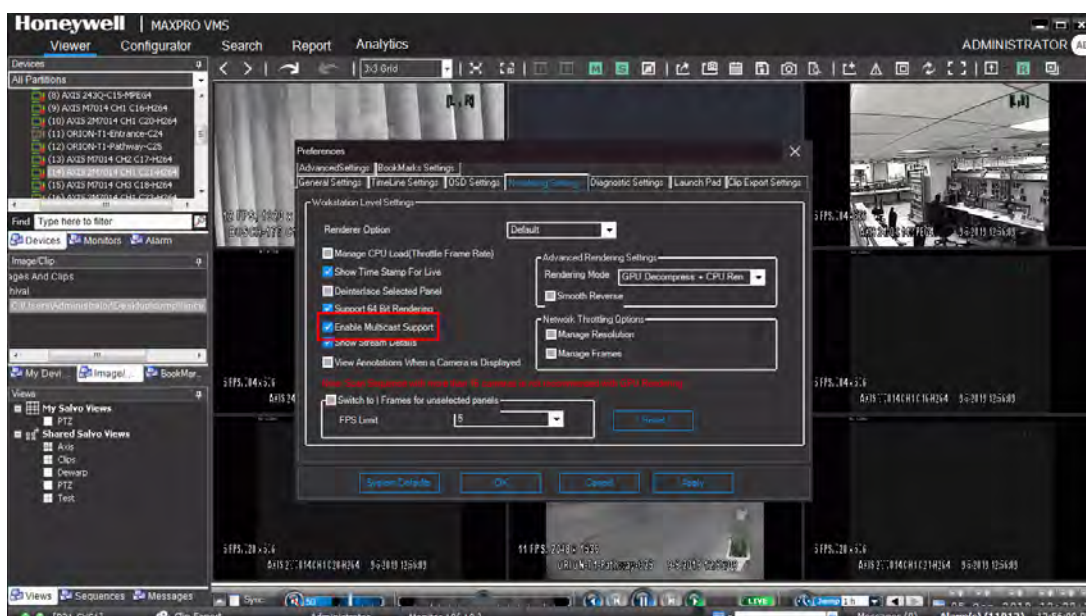


Figure 4-106 NVR Configuration

Step4 - Configuration in MAXPRO® VMS

1. In Preferences > Rendering Settings tab, select the Enable Multicast Support option as highlighted below.
2. Click Apply and then OK.



After performing the above four steps, in VMS Viewer user can identify the Multi-cast streaming cameras as [M] on the top right corner as highlighted below.



Figure 4-107 VMS Viewer

Four Eye Authentication:

This feature is also part of Privacy Protection setting and to meet the EU GDPR compliance standards easily. This is to restrict all users in a surveillance system to perform Playback operation. While performing playback operation at least two

people from different roles should authenticate. For an Administrator, authentication is not required and can perform any playback operation. However, using license; authentication for an administrator can be configured.

For a non Administrator user, by default a popup is displayed and an Administrator user or a User from some other group needs to authenticate to perform playback operation.

Note: This feature is license based and it is not supported in Viewer Edition. For R600 Enterprise Edition 60 days of trial license is applicable for both (GDPR) features. For R600 Viewer Edition these features are not available in the permanent demo license.

The following table explains the Four eye authentication based on the user and roles

User	Authenticating User	Valid Authentication
User 1[of Group 1]	User 1[of Group 2]	Yes
User 1[of Group 1]	User 2[of Group 1]	No

How to enable Four Eye Authentication

Note: Only an Administrator can provide access to this feature to an Operator.

- In the Preference Tab > General Settings, select the Enable Four Eye Authentication check box as highlighted below

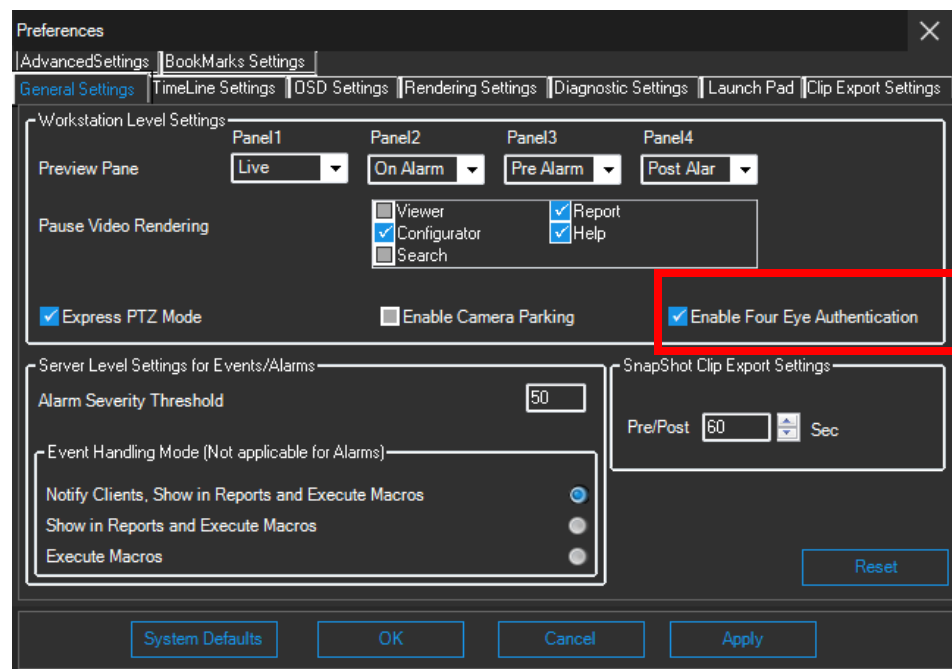


Figure 4-108 Four Eye Authentication

How Four Eye Authentication feature Works

For an Non Administrator user

1. When an Non Administrator user (Operator) tries to perform a playback operation then the following dialog box appears on th screen.

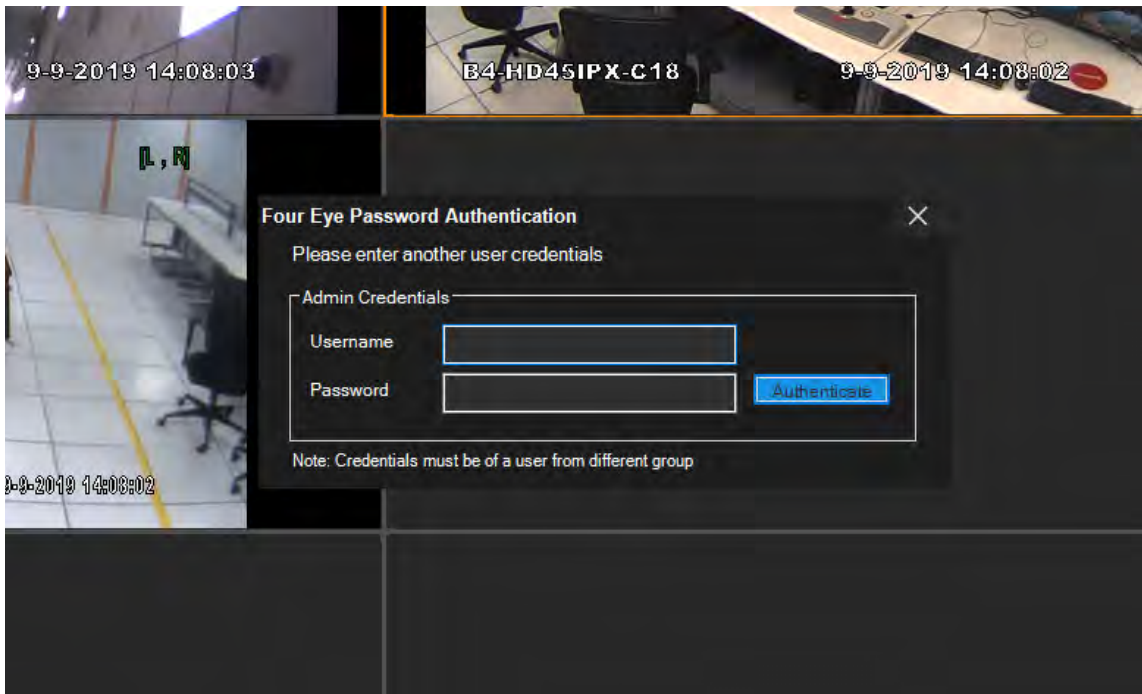


Figure 4-109 Four Eye Authentication box

2. Enter the credentials of Administrator user or a User from some other group.

Note: For authentication, the logged in user and the Administrator user should not be from the same group

The following table explains the Four eye authentication based on the user and roles

User	Authenticating User	Valid Authentication
User 1[of Group 1]	User 1[of Group 2]	Yes
User 1[of Group 1]	User 2[of Group 1]	No

3. Click the Authenticate button to view the playback video. After authentication the Four eye authenticated user and logged in user icons are displayed on the top right corner of the screen as highlighted below. For example: In the below image for Worker user, a Manager authenticates and the corresponding users are created.

- Until the four eye authenticated user is available the operator can perform any playback operation.

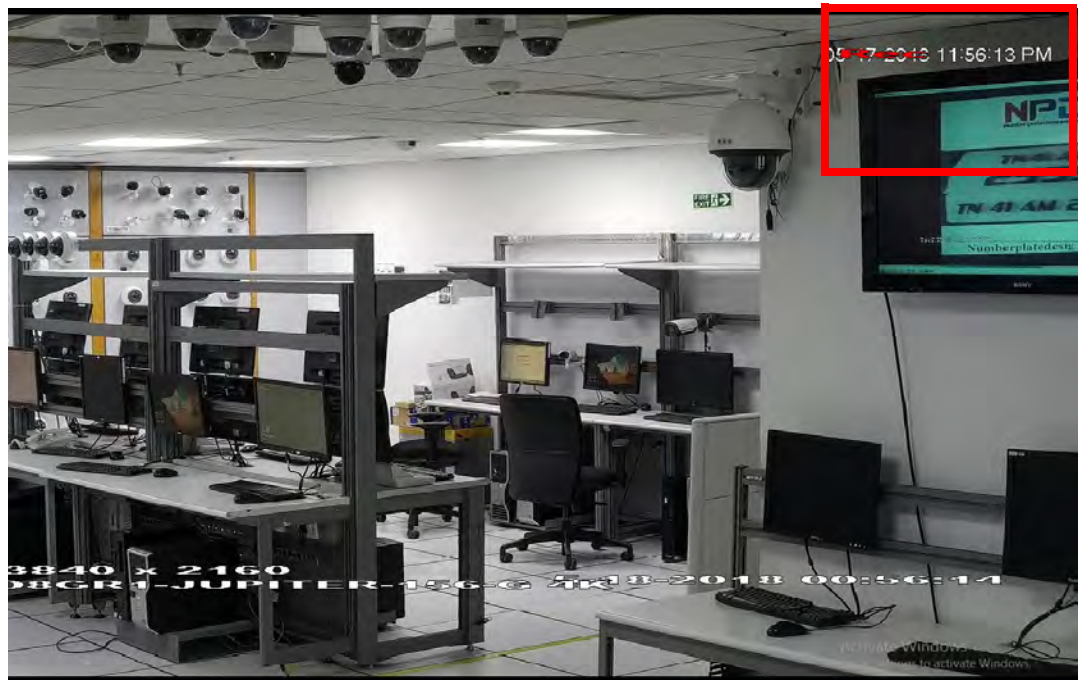


Figure 4-110 Authentication success

- If the four eye authenticated user logs off as highlighted below then again for any playback operation the Admin authentication is required.

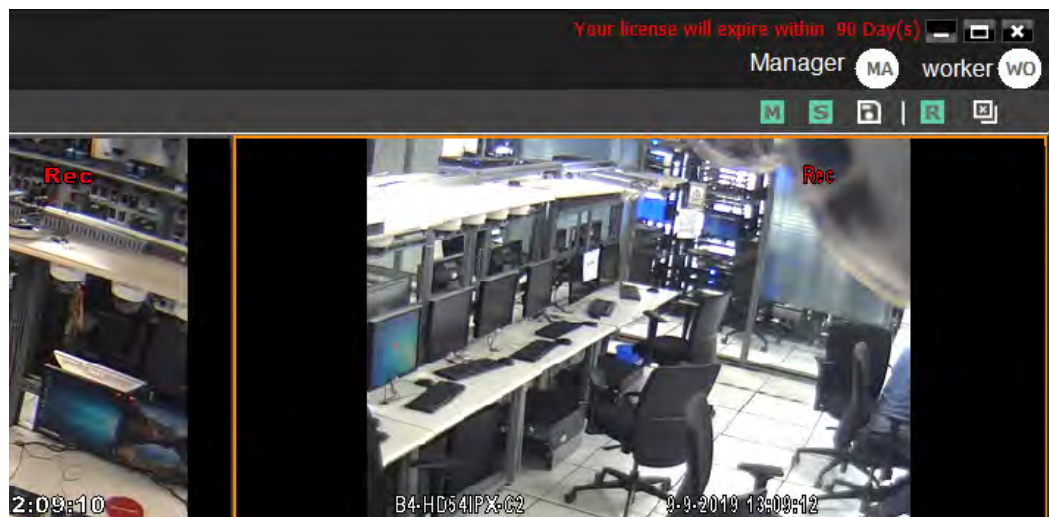


Figure 4-111 Authenticating user

VMS in VMS Enhancements

Apart from Cameras, relays and sensors user can now discover Sites, Workstations, partitions and users. This feature helps user to import all the configurations from the child VMS to Master VMS instead of reconfiguring it and hence saves time. The below screen displays the additional check box to discover Sites, Workstations, partitions and users.

As highlighted in the below image, in the Discovery Wizard a new check box is introduced to discover Partitions, Site, Workstations and Users.

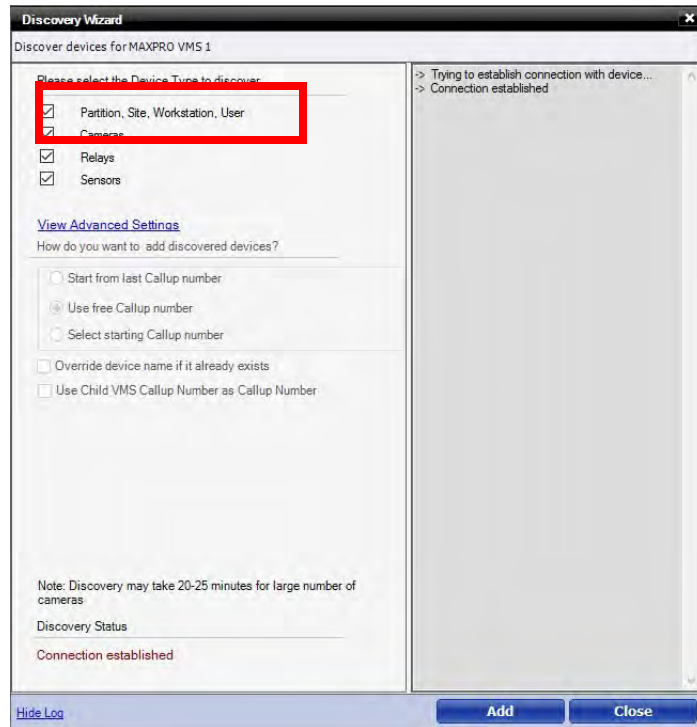


Figure 4-112 Discovery Wizard

The below image displays the discovered Partitions, Site, Workstations and Users in result pane.

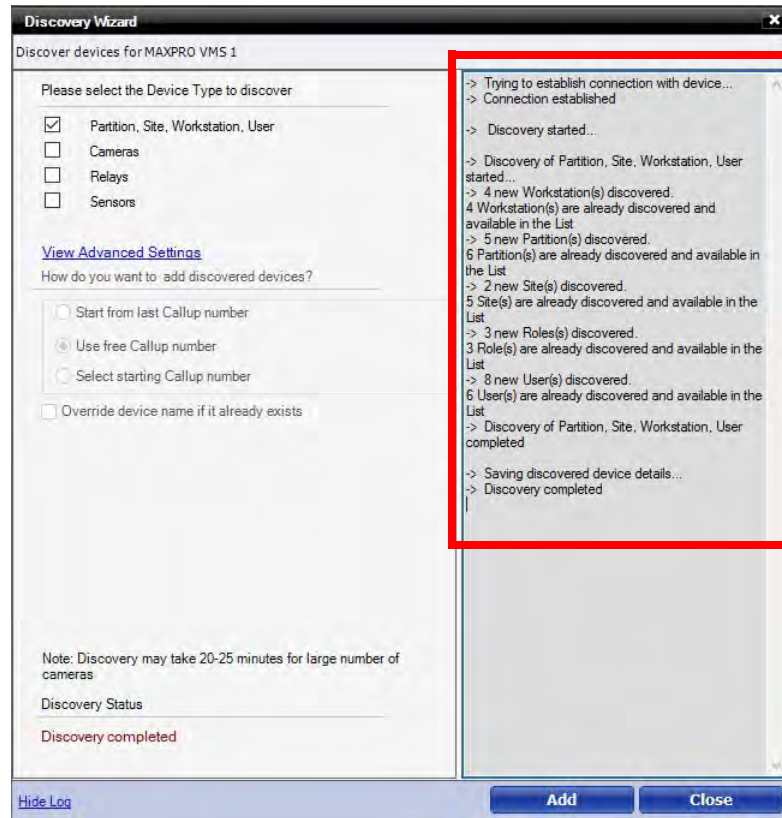
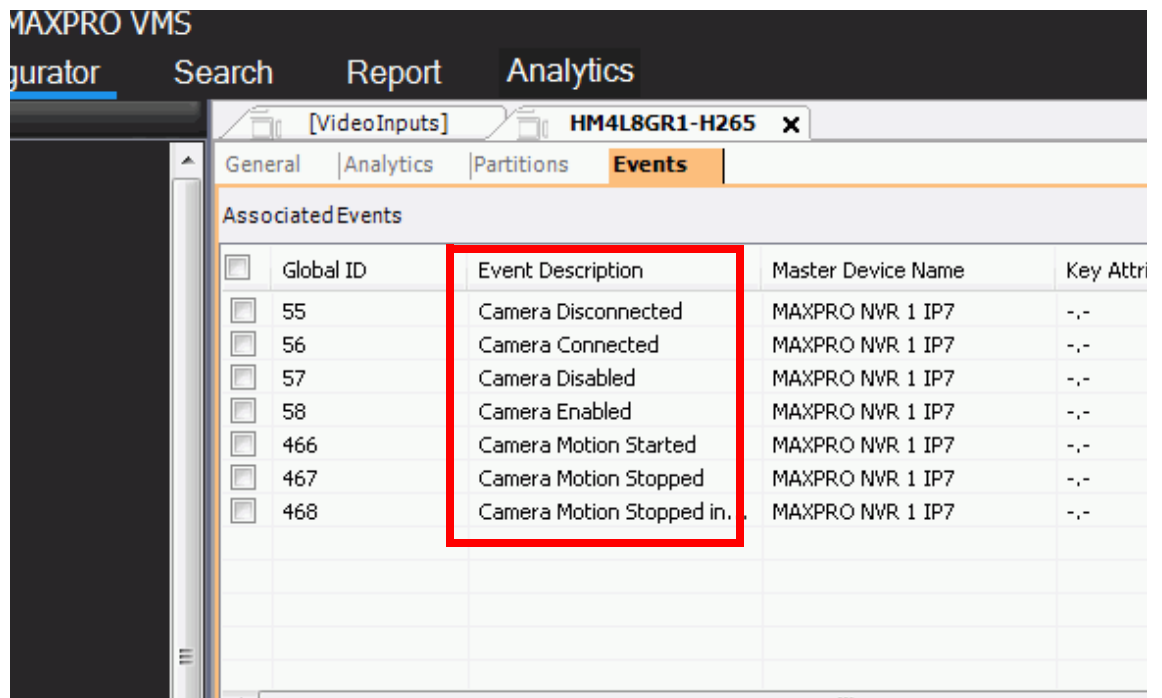


Figure 4-113 Discovery Result

Default Events Association

After upgrading to R600, if user discovers the recorders then for only newly added recorders, by default all the events will not get associated to cameras. Only few events will be associated with the devices and cameras. If user need more events to be associated then it needs to be configured manually see [Associating Events and Event Attributes to a Recorder](#) for more information.

For example below image displays the events associated by default for MAXPRO NVR Recorder. Similarly based on the recorder discovered the default events are displayed.



The following are the list of events associated by default based on the recorder discovered.

#	Event Name	Event ID
1	CAMERA_VIDEO_LOSS	1
2	CAMERA_DISABLED	21
3	CAMERA_ENABLED	22
4	DISCONNECTED	27
5	CONNECTED	28
6	CAMERA_DELETED	34
7	CAMERA_ADDED	39
8	CAMERA_VIDEOLOSS_ALARM	65
9	CAMERA_VIDEOLOSS_CONFIGURATIONFAIL ED	66
10	CAMERA_VIDEOLOSS_CONFIGURATIONOK	67
11	CAMERA_VIDEOLOSS_OK	68
12	CONNECTION_LOST	87

#	Event Name	Event ID
13	OFFLINE	93
14	VIDEO_LOST	140
15	VIDEO_RESTORED	141

Enhanced GPU Rendering

GPU Rendering capability is now enhanced to handle the camera video packets along with decompression technique. This helps the system not to depend on CPU for rendering video. User can view smooth and clear live video through GPU rendering. User should modify the registry value in client or server machine to enable GPU rendering mode.

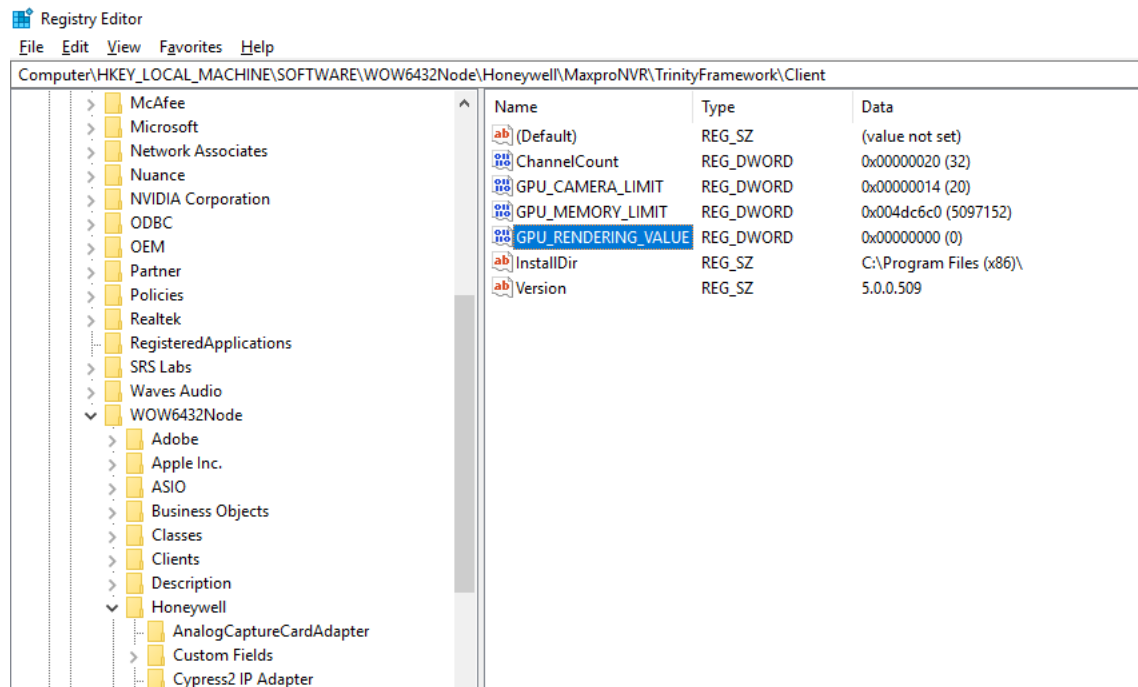
The following list of camera models/machine will not render in GPU mode:

- GrandEye Camera Models
- Dewarping Camera Models
- Anonymizaion enabled cameras
- Analog Cameras
- 32 bit processor rendering client machine

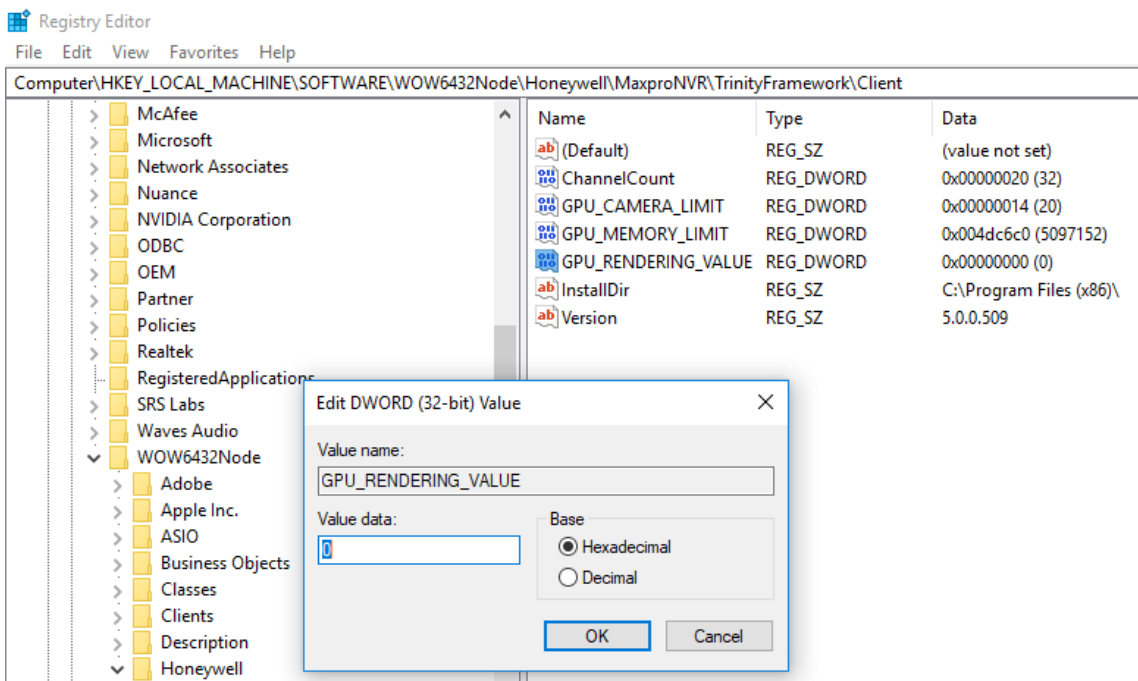
Settings for Rendering Video through GPU

Note: Ensure that user has enabled the Support GPU Rendering check box in Preferences > Rendering options tab to render video through GPU.

1. In a client or server machine, open the Registry Editor.
2. Navigate to the path
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Honeywell\MaxproNV
R\TrinityFramework\Client as shown below.



- On the left pane, double-click GPU_RENDERING_VALUE. The Edit DWORD value dialog appears as shown below.



4. Modify the value to 1 in Value data box.

Note: If the Value data flag is set to 0 then rendering will happen through CPU mode.

5. Click OK. Drag and drop the required cameras on to the panel to view the improvised GPU rendering mode.

GPU Rendering Combinations

The below table explains the combination settings between Enable GPU Rendering option and Registry settings

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

How to identify if a camera is GPU Rendering Mode

After Enabling GPU: The font will be clear and the clarity of live video will be high and smooth as shown below.



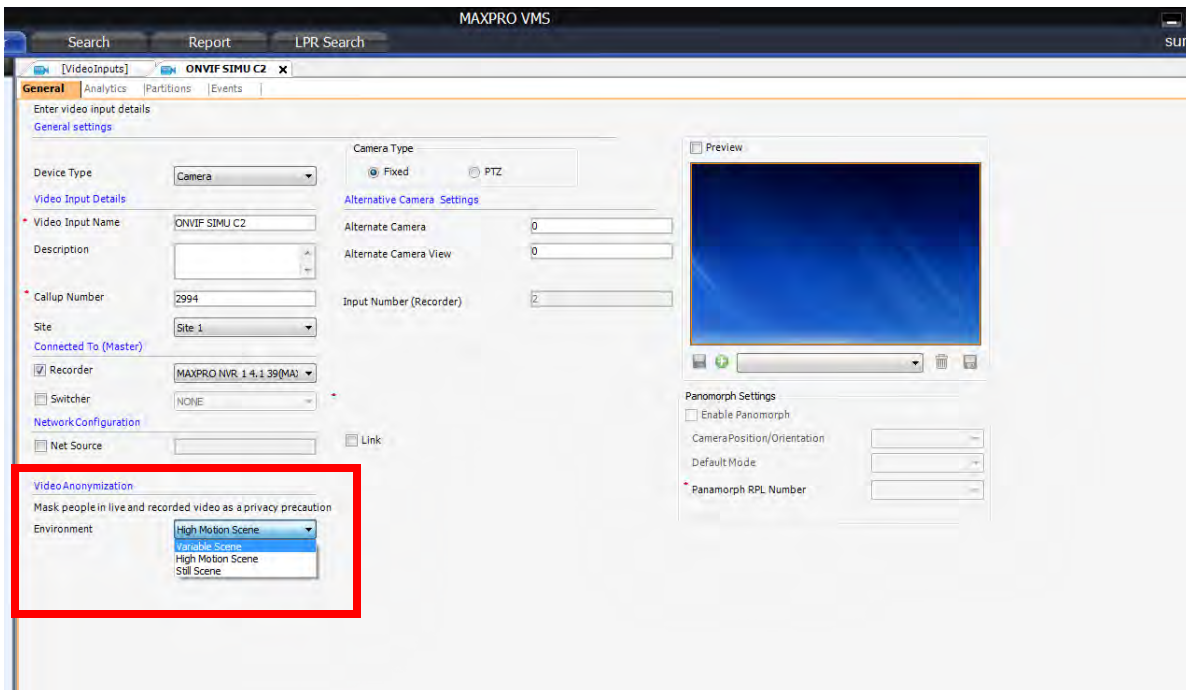
Video Anonymization

This feature allows you to configure or mask identifiable objects based on the scene environment. User need to select the required environment from the drop down list based on the camera mounting position. The following are the Environments supported in this T-Patch

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

How to Anonymize objects based on Environment

1. Click the Configurator tab.
2. Expand Devices in the navigation area, and then click Video Inputs. The Video Inputs screen appears in the display area, and displays the list of video inputs
3. Click Add. The Camera > General screen appears by default.



4. Under Video Anonymization, select the required option from the Environment drop-down list to mask people in live video scene. The available options are:

Settings	Description
Variable Scene	Select this option if the scene contains both stationary and moving people or objects.

Settings	Description
High Motion Scene	Select if you want to anonymize the objects in high motion scene
Still Scene	Select to anonymize the objects in a scene where the scene predominantly contains stationary people and objects.

Following images display the type of video anonymization scenes based on the environment selection.

For Variable Scene



For High Motion Scene



For Still Scene



Playing archived clips through Client machine

Pre-requisite

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

User needs to have the privileges to access the archived clips from remote NVR clients. Below table details out the possible combinations to play the archived clips from client machine.

Note: In Discovery Wizard, Select the Use NVR Unique System Number as Callup Number check box before discovering the devices for Archival Playback.

- Scenario 1: If user has configured Fixed drive in NVR Server For Archival.

Configured Archival path NVR Server	Then Client should have access to this path	Description
NVR Server (10.78.34.100): D:\archival	\\10.78.34.100\D\$\archival	User can access with this admin share only if the logged in user of NVR client is a local administrator in NVR server.

- Scenario 2: If user has configured shared path in NVR Server for archival then user need to configure the Archival drive as UNC path.

Configured Archival path NVR Server	Then Client should have access to this path (Read Only access)
NVR Server \\10.78.34.100\archival	\\10.78.34.100\archival

How to achieve the above Scenario 2 in Domain Environment

- NVR Server and NVR client should be added to the same domain environment

Refer the Windows specific documentation on how to configure the NVR Server and NVR client to the same domain controller.

- Add two user in the Domain Controller as mentioned below
 - Add one Domain user as the Local Administrator in NVR Server
 - Add another Domain user as a local Administrator in NVR Client (Check whether it is only local administrator or less privileges access)

How to achieve Scenario 2 in Work group

- Scenario 3: If user using NAS drive

If NVR Server Path (using NAS as archival location):	The Client path to access
\\10.78.34.200\NVR_A_ARCHIVAL	\\10.78.34.200\NVR_A_ARCHIVAL

- Scenario 4: If user using SAN then client can be accessed as mentioned in Scenario 1 above.

Annotations

Annotations support for Intrusion Trace and Loiter Trace in Live and Playback video is supported in MAXPRO® VMS with MAXPRO® NVR recorder integration. This feature helps to trace and locate the moving subjects in live/recorded video and generates an alarm if intrusion or loitering is detected.

Equip-S series camera supports Annotation feature along with Intrusion trace and Loitering Trace alarms. These alarms are in-built with Equip-S series camera and are made available by installing required analytics licenses.

Annotation with Intrusion Trace alarm: This feature helps in detecting a subject, if it enters a predefined restricted area. The system will annotate and detects the object with Green rectangular box. If the object is detected in the restricted area then the annotated Green rectangular box turns to Red and an alarm is generated.

Annotation with Loitering Trace alarm: This feature helps in detecting an object If loitering beyond the specified duration of time in a predefined region. The subjects is bounded by the box along with the duration (time in seconds) for which it is identified in the region of interest. If the subject is loitering in the region beyond a predefined time then the annotation boxes turns to Red and an alarm is generated.

See [Enabling Annotations in VMS](#) on page 361.

Note: Currently Annotation feature works with only with old GPU rendering modes.

Annotation feature is supported with the following camera models and firmware version

S.No	Camera Model	Firmware	Loiter	Intrusion
1	H4D8GR1	2.420.HW00.9, Build Date: 2018-12-17	V1.20.60	V1.20.60
2	HCD8G			
3	HBD8GR1			
4	HFD6GR1	1.000.HW00.9, Build Date: 2018-12-17	V1.20.60	V1.20.60
5	HFD8GR1			
6	HDZ302DE	1.000.0043.3, Build Date: 2019-01-07	V1.20.60	V1.20.60
7	HDZ302D			
8	HDZ302DIN			

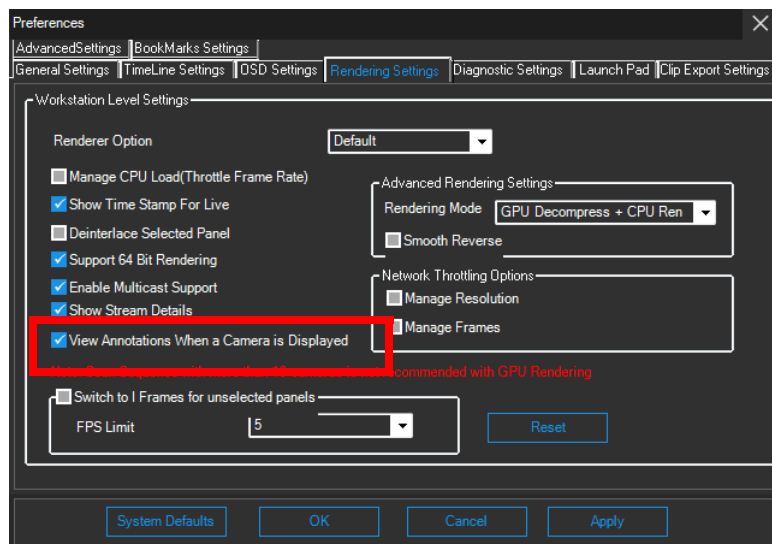
Configuring Annotations

Refer to the [MAXPRO® NVR Installation and Configuration Guide](#) for the complete details on configuring Annotations at camera level and at NVR level.

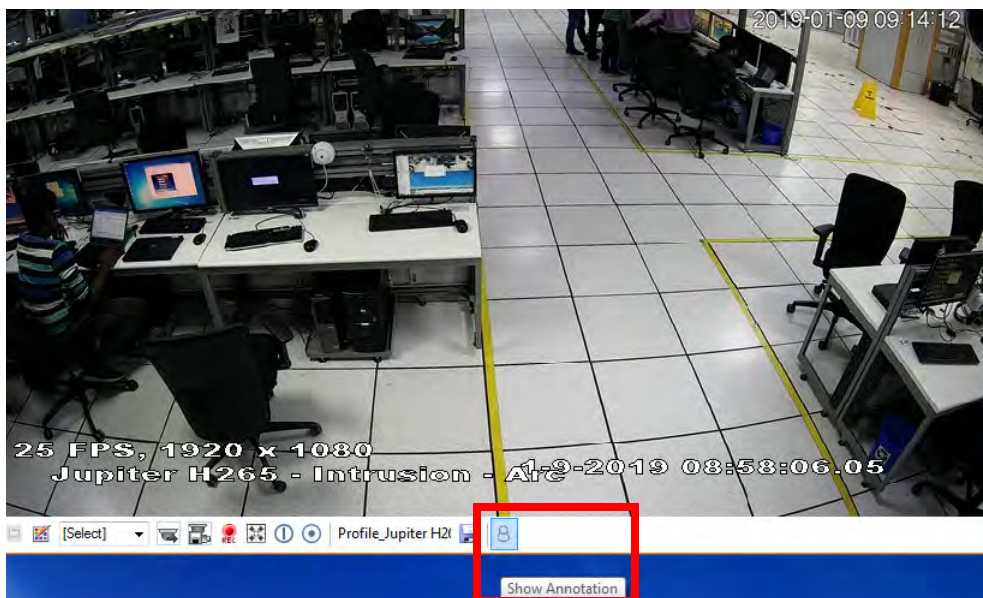
Enabling Annotations in VMS

In Preference

- In Preference > Rendering Setting tab, select the View Annotations when a camera is displayed check box to enable annotations for all the supported cameras (Equip-S Series)



- In Video panel, hover the mouse in the bottom of the panel to view the options and then click on Show Annotations icon for that particular camera as highlighted below. You can also click the same icon to Hide annotations only for that camera.



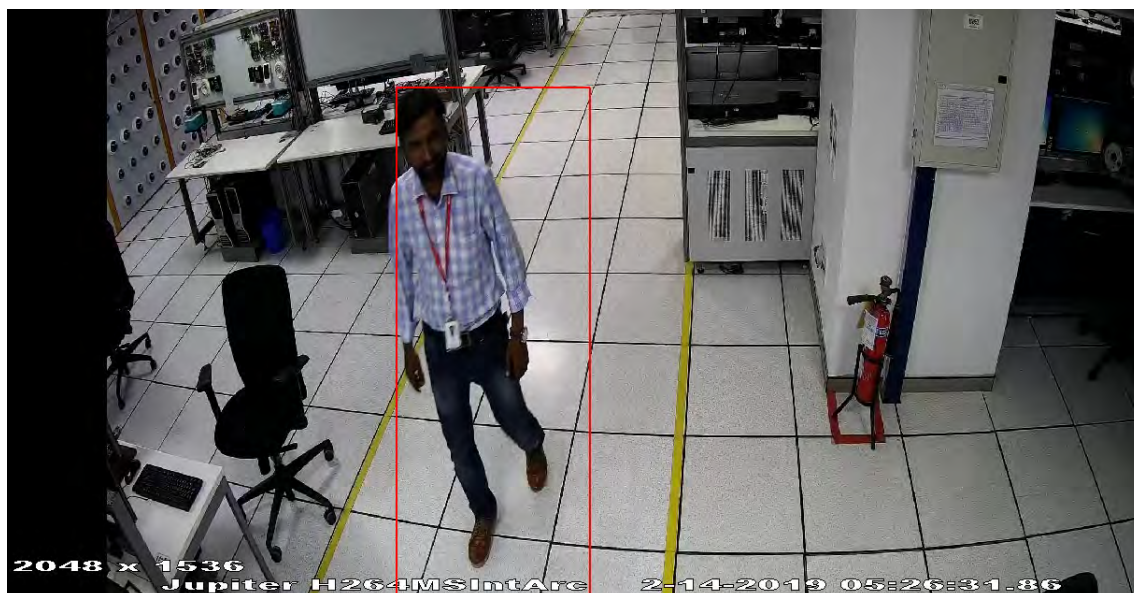
Annotation with Intrusion Trace in VMS (Live/playback)

After the Annotation feature is enabled for Intrusion trace, rectangular bounding boxes will be accompanied with any moving object in the scene. If any object is moving within the predefined area then the object is highlighted with Red rectangular box and an alarm is generated as shown below.

Annotation with Intrusion Trace (Live) without alarm



Annotation with Intrusion Trace (Live) with alarm



Annotation with Intrusion Trace (Playback) without alarm



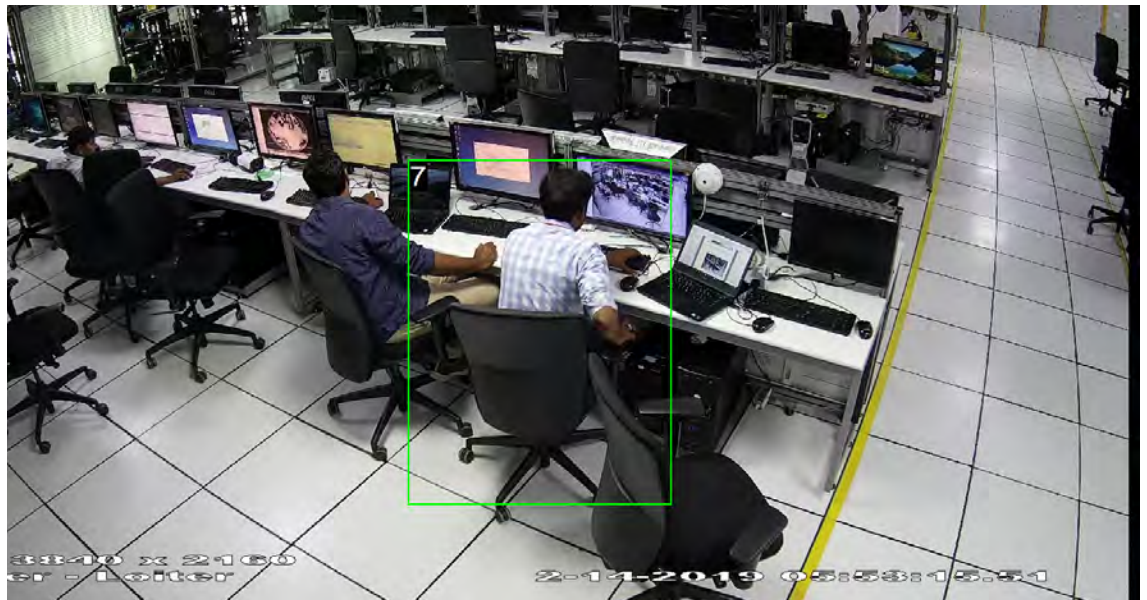
Annotation with Intrusion Trace (Playback) with alarm



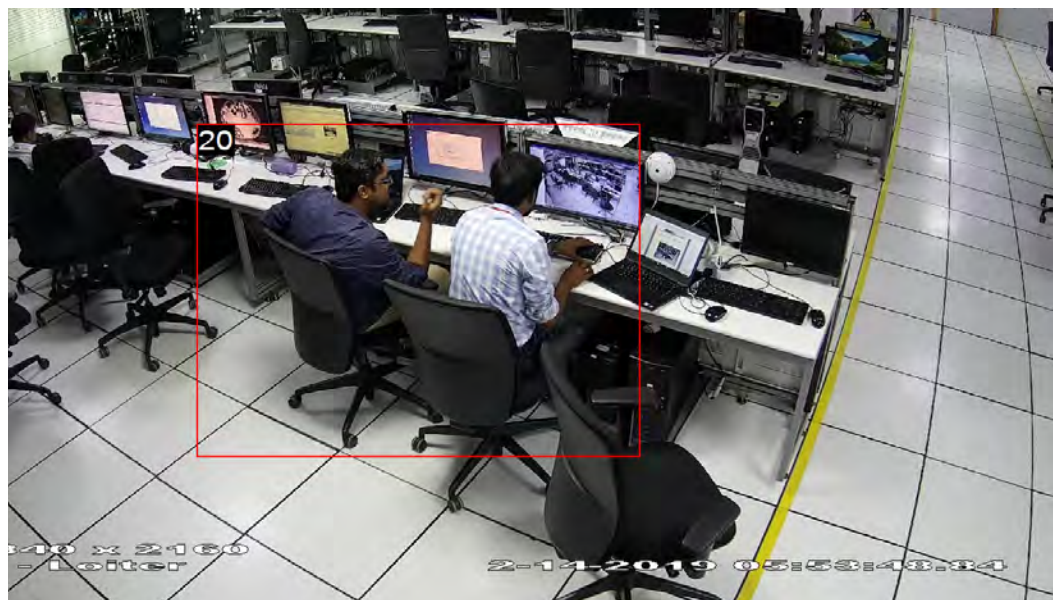
Annotation with Loitering Trace in VMS (Live)

If an object loiters within the predefined zone then a Green colored rectangular bounding box is displayed. If the same object loiters beyond the Maximum Loitering Time, then the object will be highlighted with a Red Rectangular box as shown below.

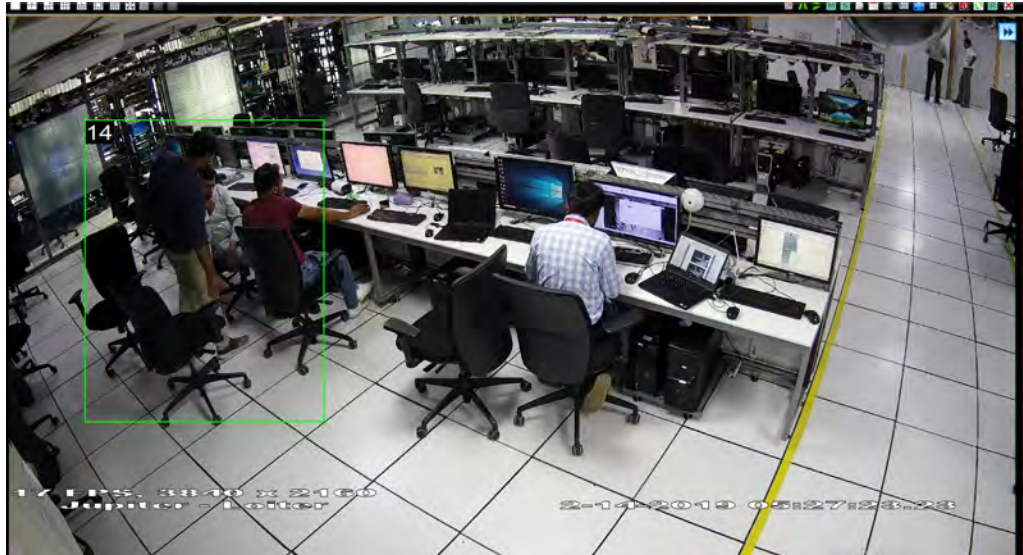
Object within the Maximum Loitering Time (Live)



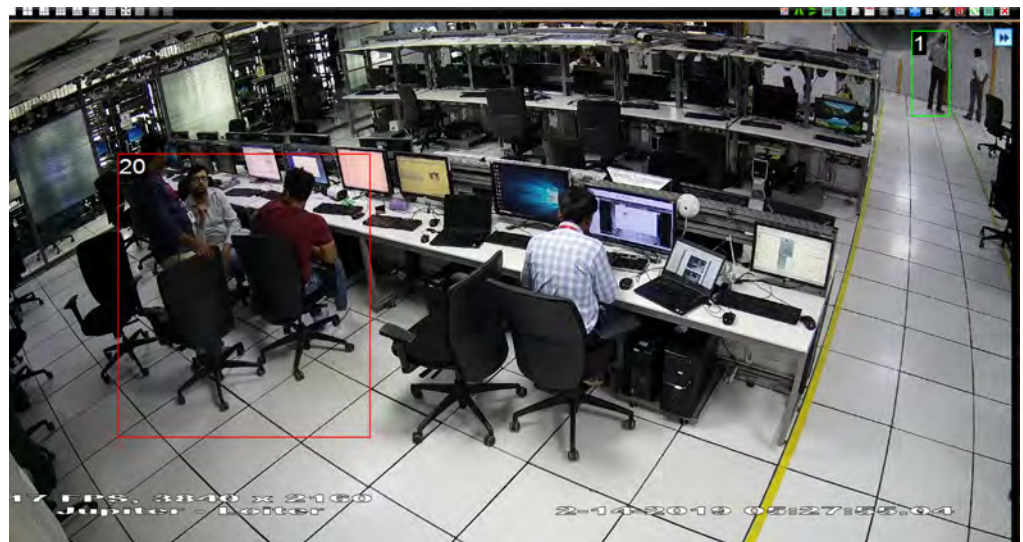
Object beyond the Maximum Loitering Time (Live) with alarm



Loitering Trace in Playback without alarm



Loitering Trace in Playback with alarm



Snapshots with Annotations

Capturing snapshots with Annotation bounding box in Live and Recorded video is supported. User can find the captured snapshots under Snapshots/Clips pane.

ADPRO XO Recorder Integration Support

ADPRO XO Recorder integration is now supported in MAXPRO VMS R550 and above version. In MAXPRO VMS user can avail the features of XO recorder including the Annotation bounding boxes. User needs to update with new license to avail the features of XO recorder in VMS.

Note: Honeywell recommends you to change the default username and password after the first login.

The following are the qualified XO Recorder models and the Firmware versions supported with MAXPRO VMS R550.

#	XO Recorder Model (Version)	Firmware Version
1	ADPRO IFT	IFT
		IFTE
2	Fast Trace 2	XO 04.02.0010
3	ADPRO IFT Gateway	XO 04.02.0012

Following are the features supported with ADPRO XO Recorder integration.:

#	Features Supported
1	Add/delete/modify AdproXO recorder in VMS
2	Discover Cameras, Relays and Sensors
3	Live Video
4	Multi Stream
5	Snapshot save, digital correction, Mirror and Flip.
6	PTZ operations
7	Playback Operations Note: Reverse playback operation is not supported. Playback operation may start a few seconds behind the selected time because of GOP settings.
8	Camera Status/Alarms
9	Events Search
11	HVA

Recommendations to configure ADPRO Recorder

Clip Export

- While exporting a clip in MAXPRO VMS with XO recorder integration ensure that you put the VMS server on the same subnet as the XO Device.

Export HBOX clip player with clips

MAXPRO VMS integration with ADPRO XO recorder allows user to export clip (HBOX format) along with the HBOX clip player. A clip player extractor.exe file is exported to the defined path and user can execute the exe to view the video. This helps the user to play the clip in any machine without depending on supported clip format player. Refer to the [MAXPRO® VMS Operators Guide](#) on how to export a clip in HBOX format.

Playback associated videos for Input Alarms

This feature enables user to playback the associated video with input alarm. User can view the video for an input alarm from all the associated cameras. This feature is support only from ADPRO XO recorder integration with VMS. Refer to the [MAXPRO® VMS Operators Guide](#) on how to view the associated videos of input alarms.

Advanced Rendering Settings

This feature provides flexibility to select different rendering combinations between CPU and GPU modes for decompression and rendering process. Earlier GPU Rendering capability was available to handle the camera video packets along with decompression. With Advance Rendering settings user can choose to distribute the load on CPU and GPU accordingly. This helps the user to improve the rendering performance of the system. The available options are

- CPU Decompress + CPU Render: This option executes low performance because entire video rendering process will be on CPU. This option is for debugging purpose and is recommended not to be selected.
- GPU Decompress + CPU Render: By default this option is selected and decompression/rendering process is shared between GPU and CPU.
- GPU Decompress + GPU Render: This option is for high resolution cameras and for cameras with 60 FPS on 4K monitors. Selecting this option may reduce the number of cameras but the video quality will be best.

Note: GPU Decompress + GPU Render option has some limitations such as Flip/Mirror/Digital corrections features may not be supported.

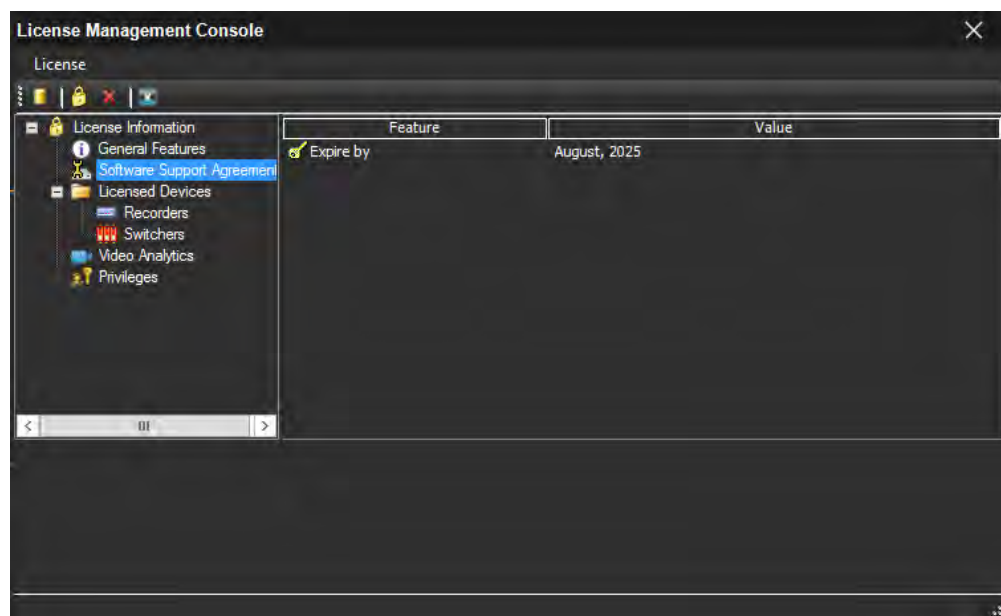
SSA – Software Service Agreement for MAXPRO

Software Service Agreement (SSA) is a flexible version specific licensing process which allows a user to get the support on the MAXPRO VMS licenses across multiple versions. From R600 release user need to buy a valid license for R600 to upgrade or for fresh installation. In addition user can buy SSA support license for a specific duration which helps to get support from Honeywell.

Please contact Honeywell Customer support. See the back cover for the contact information in respective regions.

Note: License is valid only for a specific release. When applied, on a incompatible version, the license will not be accepted. For example if you install R500 license on a R600 installed machine, then a message **Selected license is invalid for MAXPRO VMS R600. Please select correct license file** is displayed.

To install the procured license refer to the 800-26005-A_MAXPRO™ VMS R600 Operator's Guide for more information. Once the SS A license is procured and installed, the License console Management window displays the SSA info entry as shown below.



License Plate Recognition (LPR)

Enhancements has been made in LPR feature to support events with cropped images, categorization and details pane. LPR scans can be monitored through a dedicated window in MAXPRO thick client. This new windows also supports filtering and searching events based on camera and category (White/Black listed/unknown).In addition you can also view the specific event video from the LPR feed.

Note: *Cropped image is displayed in report if NVR and camera is in latest version of MAXPRO version. In addition, the camera firmware should also be in latest version dated 17-06-2019. In older version of NVR or camera the report is displayed without cropped images.*

Following are the enhancements in LPR tab:

- New dedicated tab for LPR event monitoring
- Search LPR events
- Filter LPR events
- Viewing, acknowledging and clearing blacklisted and white listed alarms in VMS Alarm viewer
- Viewing video from Alarm window
- Live LPR view
- Details pane
 - Cropped Image of the license plate
 - Camera Name
 - Event Date and Time
 - Geographical location details
 - Category details such as White Listed.Black Listed and Unknown with varying color
 - Confidence Level: The maximum percentage value that a number plate is matching with the specific category
 - Recorder Name
 - Site Name

Note: *Arabic number plates are also supported in English OS with Arabic locale*

Pre-requisite Study

To configure and use the LPR feature in MAXPRO VMS and NVR, refer to the 800-24023-A_MAXPRO_ LPR_User Guide.

LPR - Viewing Persona Based Events

In R600 release LPR camera and events can be configured and viewed by a specific user based on the privileges granted. Earlier all the LPR alarms are displayed to logged in user irrespective of user privileges. In R600 user need to configure partitions and associate the required cameras to the partitions. These partitions can be assigned to specific user. The user will only be able to monitor the associated camera and the events accordingly.

NDAA Series 30 camera Integration in MAXPRO NVR & VMS

Series 30 Camera integration is supported in R600 release with MAXPRO NVR recorder. The following tables explain the list of supported camera models, firmware version and events.

Note: HC30WF5R1 model camera does not support HTTPS.

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

Supported Events

The following events are support with Series 30 Camera Integration.

Event
Motion Detection
Tamper
Image too blur

Image too dark
Image too bright
People Detection
Intrusion

Supported key Features

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

Secure video communication with Series 30 Cameras

Refer to the 800-25609-A_Honeywell 30 Series IP Cameras Network Security Guide for complete details.

MPEG2 Encoder Support with MAXPRO NVR and VMS

R600 supports legacy MPEG2 Encoders with Live and playback, Alarms and VMS in VMS functionalities. The following encoders are supported.

- ENC8M2
- VE8M2

Supported Firmware Version: 1.2.261

Supported Features are:

- Alarms
- VMS in VMS
- Live
- Playback
- Export
- Only Multi casting streaming address

Video Guard service for SIRA compliance

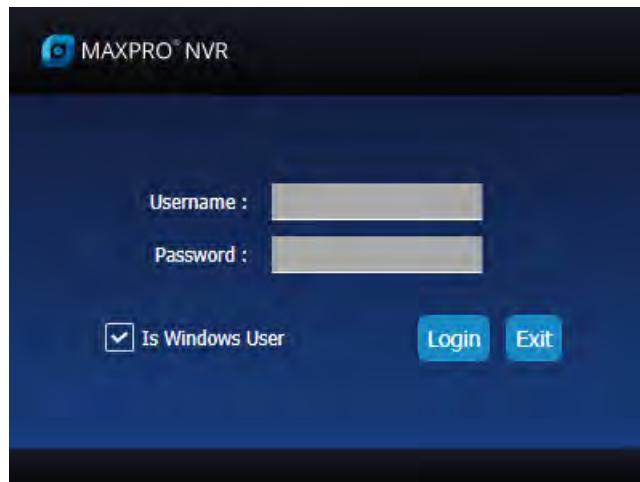
MAXPRO R600 release supports SIRA compliance with Video Guard Device Integration. This is to meet the specifications defined as part of the City wide Surveillance initiative by the Security Industry Regulatory Agency (SIRA) of Dubai, UAE, and being adopted across Middle-East countries.

User can run this service in NVR box to be in compliant with SIRA standards. To enable the service user needs to use MAXPRO Video Guard Configurator available in Bin folder. This configurator connects to MAXPRO NVR, sends the recorder information to video guard systems and synchronize the heartbeat messages (Polling) and system time.

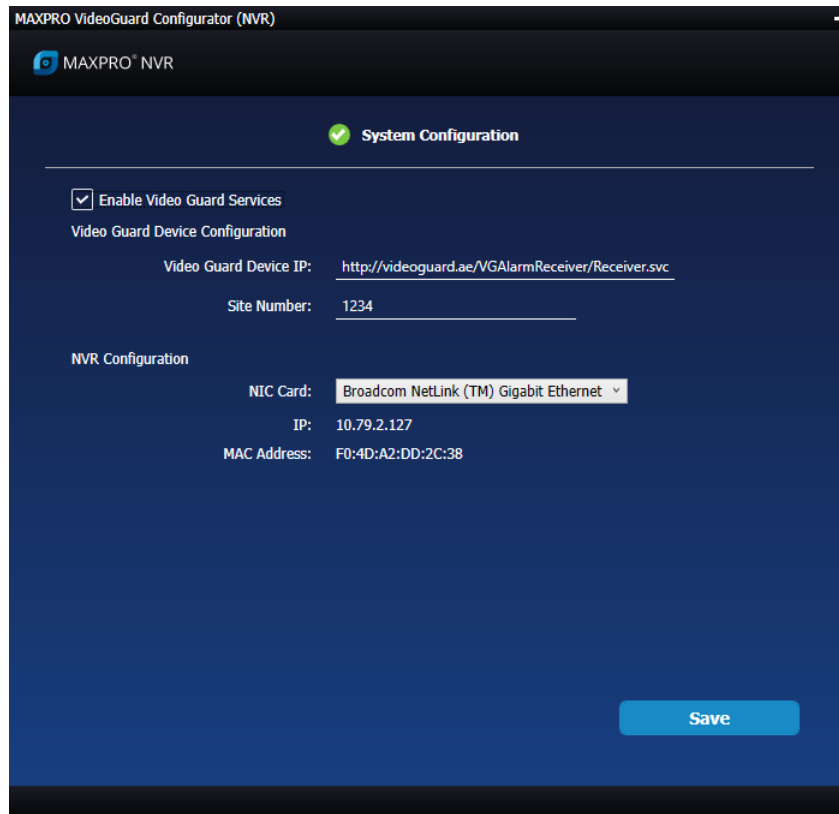
Note: *Network time sync should be disabled when NVR is configured to communicate with Video Guard device.
It is required to restart NEO engine after Video Guard Service changes the timezone.*

How to run the WCF service using MAXPRO Video Guard Configurator

1. Navigate to MAXPRO NVR Bin folder and then locate the MAXPRO Video Guard Configurator.exe.
2. Double-click the exe. A login window is displayed as shown below.



3. Type the Username and Password in the box provided.
Or
Select Is Window User check box to login using windows credentials.
4. Click the Login button. The MAXPRO Video Guard Configurator application is displayed as shown below.



5. Select the Enable Video Guard Services check box. By default it is cleared.
6. Under Video Guard Device Configuration:
 - Type the Video Guard Device IP
 - Type the Site Number
7. Under NVR Configuration:
 - Select the NIC card from the drop down list
8. Click the Save button.

People Counting Dashboard Utility

VMS Occupancy Dashboard Utility allows you to track the number of people entered or exited from a specific area or premises or pathway. This utility helps to manage the space in commercial buildings to take appropriate actions based on the number of people entered or exited. The Occupancy Dashboard displays the Occupancy Summary and Trend based on the cameras configured and duration. This utility needs to be used along with MAXPRO VMS and HVA.

The actions are:

- Monitoring/Managing parking area/building
- Space management in big stadiums/shopping mall

VMS Occupancy Dashboard Utility contains two parameters as explained below:

- Configuration
 - Configure Data Source: Allows you to setup database to connect the Trinity database. User can login through Windows authentication or install the SQL server standalone to connect.
 - Group Devices: Allows you to manage camera groups such as associate/disassociate cameras, create new camera group.
- Overview
 - Occupancy Dashboard: Displays the occupancy summary and trend with real time data in graphical format based on duration.

Configurations

The VMS Occupancy Dashboard Utility configuration includes the following:

1. Configuring the HVA in VMS
2. Configure the Data Source
3. Configure or Group the Devices
4. Viewing the Occupancy Dashboard. Refer to the MAXPRO VMS R630 Operators Guide.

Configuring the HVA in VMS

Perform the steps as explained in the below sections:

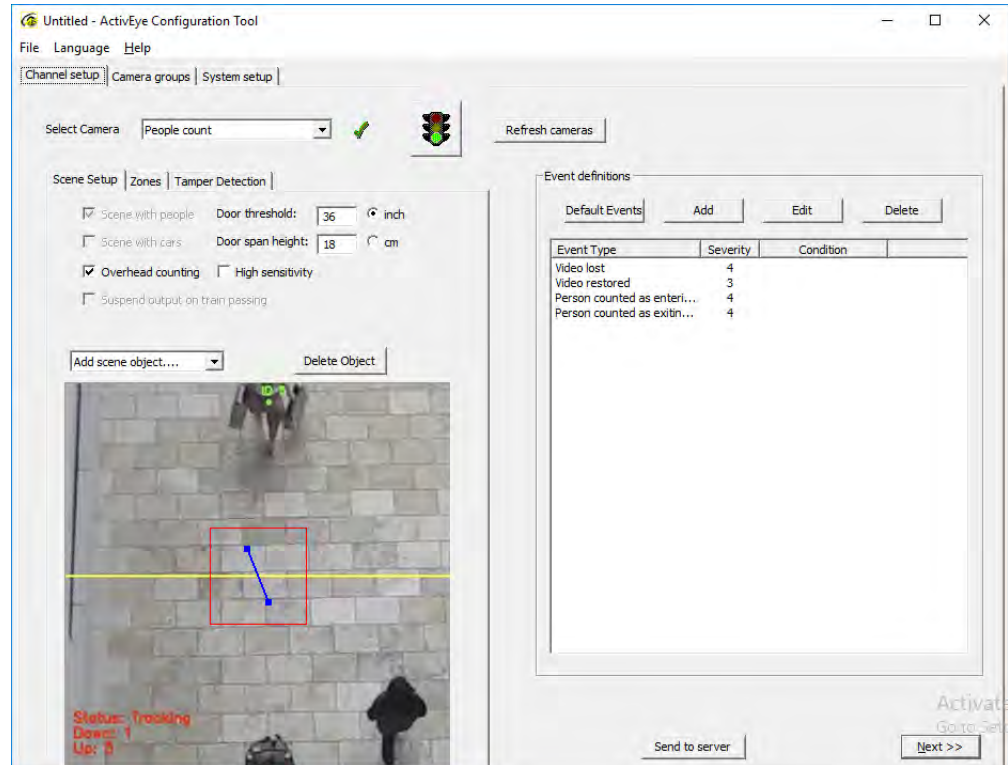
Step 1: [Adding an Analytics Server](#)

Step 2: [Associating Events and Event Attributes to Analytics](#)

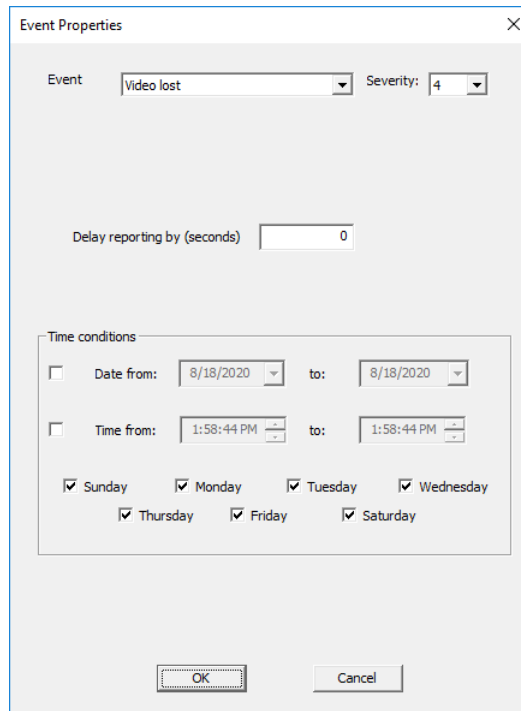
Step 3: Setting the Video Analytics (ActivEye) Configuration Tool

After performing the above steps, perform the below procedure to configure the people counting configurations on the selected camera.

1. Click Launch HVA Configurator link. The ActivEye Configuration Tool screen is displayed as shown below



2. Under Channel Setup > Scene Setup, select the Overhead Counting check box.
3. From the Add Scene Object drop-down select Add door threshold or Add door span at fixed height options based on the requirement.
4. Click the Zones tab and then add the required zone from the drop-down list.
5. Select Counting Line option from the Zones drop-down list.
6. Under Event Definition, click the Add tab. The Event Properties dialog box is displayed.



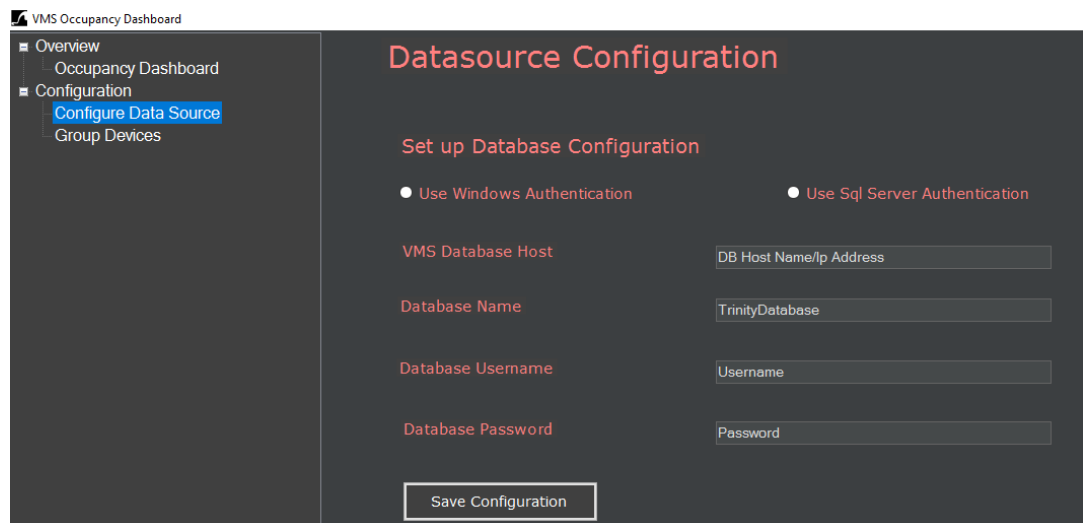
The 'Event Properties' dialog box contains the following fields and options:

- Event:** A dropdown menu with 'Video lost' selected.
- Severity:** A dropdown menu with '4' selected.
- Delay reporting by (seconds):** A text input field with '0' entered.
- Time conditions:** A section with two rows of date and time pickers, each preceded by an unchecked checkbox.
 - Row 1: 'Date from: 8/18/2020' and 'to: 8/18/2020'.
 - Row 2: 'Time from: 1:58:44 PM' and 'to: 1:58:44 PM'.
- Days of the week:** A set of seven checkboxes, all of which are checked: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

7. Select the required event from the Event drop-down list.
8. Set the even Severity to 4 and then click OK.
9. Click Send to server to complete the configuration.

Configuring the Data Source

1. Navigate to C:\Program Files (x86)\Honeywell\TrinityFramework\Bin\OccupancyDashboardUtility and then click Trinity.Occupancy.Viewer.Utility.



The 'VMS Occupancy Dashboard' application window shows the 'Datasource Configuration' screen. The left sidebar has a tree view with 'Overview', 'Occupancy Dashboard', 'Configuration', 'Configure Data Source' (highlighted), and 'Group Devices'. The main area is titled 'Datasource Configuration' and contains the following elements:

- Set up Database Configuration:** Two radio buttons: 'Use Windows Authentication' (selected) and 'Use Sql Server Authentication'.
- VMS Database Host:** A text input field with 'DB Host Name/Ip Address' entered.
- Database Name:** A text input field with 'TrinityDatabase' entered.
- Database Username:** A text input field with 'Username' entered.
- Database Password:** A text input field with 'Password' entered.
- Save Configuration:** A button at the bottom.

2. Click Use Windows Authentication option to login using widows credentials.
Or
Click Use SQL Server Authentication option to login using the SQL server credentials. In this case user need to install the SQL separately.
3. Type the following:
 - VMS Database Host: Type the DB Host Name / SQL Instance name.
 - Database Name: This is the TrinityDatabase.
 - Database User Name: Type the user name which you have entered while installing SQL server
 - Database Password: Type the password which you have entered while installing SQL server
4. Click Save Configuration

Configuring or Group the Devices

1. Click the Group the Devices node on the left pane of VMS Occupancy Dashboard Utility. The Manage Camera Groups screen is displayed.



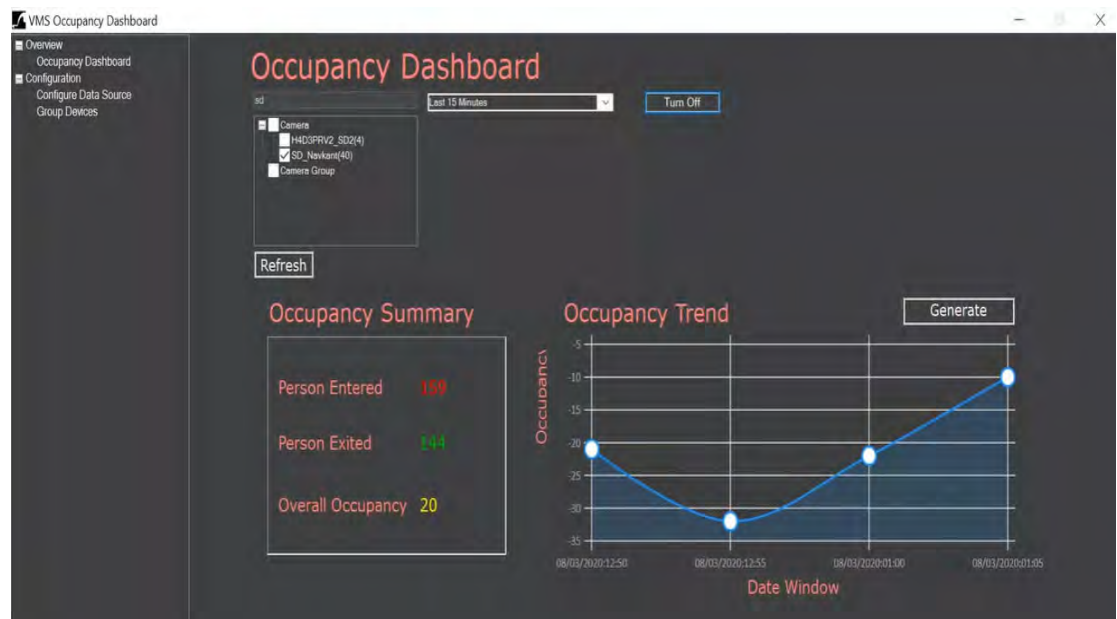
To create a new camera group:

- a. Under New Camera Group click Refresh to view the configured cameras list. Alternatively you can search the cameras. The list of configured camera displayed.
- b. Select the required cameras and then click the > button to move under Selected Devices area. Alternatively you can click the >> button to move all the cameras at once.
- c. Enter a new name for the selected camera group and then click Create.

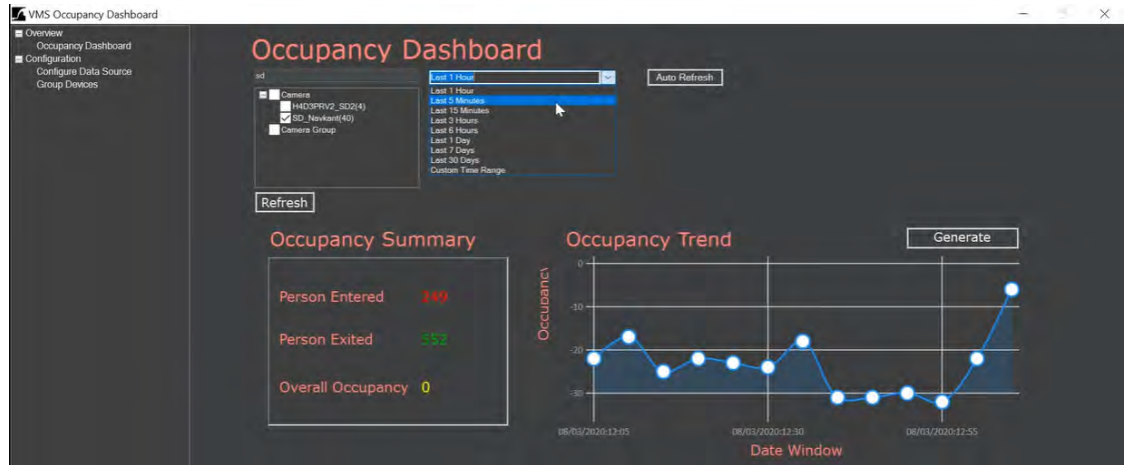
2. Under Camera Groups, click the Refresh button to view the configured camera groups.
3. Select the Group the associated cameras are displayed under Associated Camera area.
4. To delete the group, select the required camera group and then click Delete Group.
5. To remove the selected camera from the group, under Associated Cameras select the required camera from the group and then click Remove Selected.

Viewing the Occupancy Dashboard

1. Ensure you have configured the following before viewing the occupancy dashboard.
 - [Configuring the HVA in VMS](#)
 - [Step 3: Setting the Video Analytics \(ActivEye\) Configuration Tool](#)
 - [Configuring the Data Source](#)
 - [Configuring or Group the Devices](#)
2. Under Overview, Click Occupancy Dashboard node. The Occupancy Dashboard is displayed on the right pane. All the camera and groups configured are displayed.
3. Select the required camera under a group or select the camera group. The Occupancy Trend and Occupancy Summary is displayed as shown below.



4. Select the required duration (In Minutes, Hours, Days and Custom Date) from the drop-down list. The Occupancy Trend graph and the Summary is displayed accordingly as shown below.



Tips:

- Click Refresh to refresh the camera list.
- Click Auto Refresh to refresh the camera and duration accordingly.

VMS in VMS support for Mask and Social Distancing Detection

MAXPRO VMS R630 release supports Mask and Social Distancing Violation Detection support for VMS in VMS scenario with Bounding boxes. User can view bounding boxes in both Master and Child VMS recorders. This enhancement allows user to track the Mask and Social Distancing alarms and events in wide range of recorders

For Master VMS both Alarm and events along with attributes are supported. For Child VMS attributes are not supported.

User need to enable View Annotations in Preference dialog box after configuring VMS in VMS. A typical example of how VMS in VMS scenario looks with Bounding boxes is shown below

Faster Drag and Drop for MAXPRO NVR cameras in MAXPRO VMS client

The time taken for the video to render in VMS client after drag and drop on to the video panel has been considerably improved. This feature requires a configuration to be enabled.

To enable this feature user need to configure the values in config files based on 32/64 bit rendering modes.

For 32 -Bit Rendering Mode:

1. Navigate to C:\Program Files (x86)\Honeywell\TrinityFramework\bin\ Trinity-RenderingServer.exe.Config.
2. Locate the CacheNeoDevice/CacheTSSDevice parameters. By default it is set to false.

3. Change it to True to enable faster drag and Drop.
4. Re-Launch the MMShell.

For 64 -Bit Rendering Mode:

1. Navigate to C:\Program Files (x86)\Honeywell\TrinityFramework\bin_x64\TrinityRenderingServer_x64.exe.config.
2. Locate the CacheNeoDevice/CacheTSSDevice params. By default it is set to false. Maximum 50 can be added in Registry.
3. Change it to True to enable faster drag and Drop.
4. Re-Launch the MMShell.

To Set the Device Cache

If you want to increase the number devices supported per recorder based on the site requirement then perform the following:

To view the current limit:

1. Navigate to C:\Users\Administrator\AppData\Roaming\Honeywell\Cache,
2. Open DeviceCache.json file and then check the limit. By default it is set to 10.

To increase the limit:

1. Navigate to C:\Program Files (x86)\Honeywell\TrinityFramework\bin\MMShell.exe.Config.
2. Change the limit based on the requirement.

Scalable Analytics Server

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

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

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

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

Converting a NVR Machine to a Analytics Remote Server

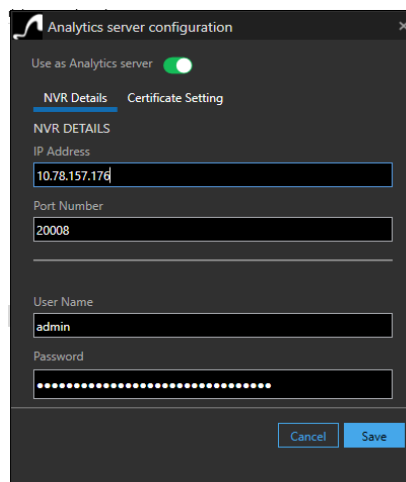
Any NVR machine can be converted into a Remote Analytics server to balance the analytics camera load on CPU. User need to ensure the below to convert a NVR machine to Analytics Server

- It should be an NVR machine without cameras. No cameras should be added
- All Neo services should be in stop state to minimize the load on analytic server.
- If you are using remote analytics servers, then ensure to enable encryption in remote analytics box as well. It is recommend to use different certificates for encryption. See [How to Encrypt the Remote Analytic Server](#) section.

In order to do ease the above steps for user, MaproNvrAnalyticServerConfigUtility is introduced. User can configure this in Remote machine to convert it to analytics server machine.

How to configure Analytics Server

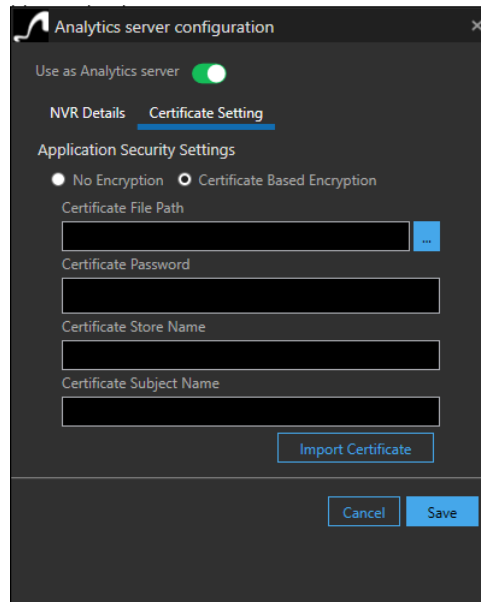
1. In Remote NVR machine, navigate to NVR Bin folder and locate MaproNvrAnalyticServerConfigUtility.
2. Run the Utility in Administrator mode. The Analytics Server Configuration dialog box appears.



3. Click the “Use as Analytics Server” toggle button to enable.
4. Under NVR Details, type the following details as explained below:
 - IP Address: This is IP address of the NVR machine where analytic cameras are added
 - Port Number of the NVR machine
 - User name and Password of the NVR machine
5. Click Save to complete the configuration.

How to Encrypt the Remote Analytic Server

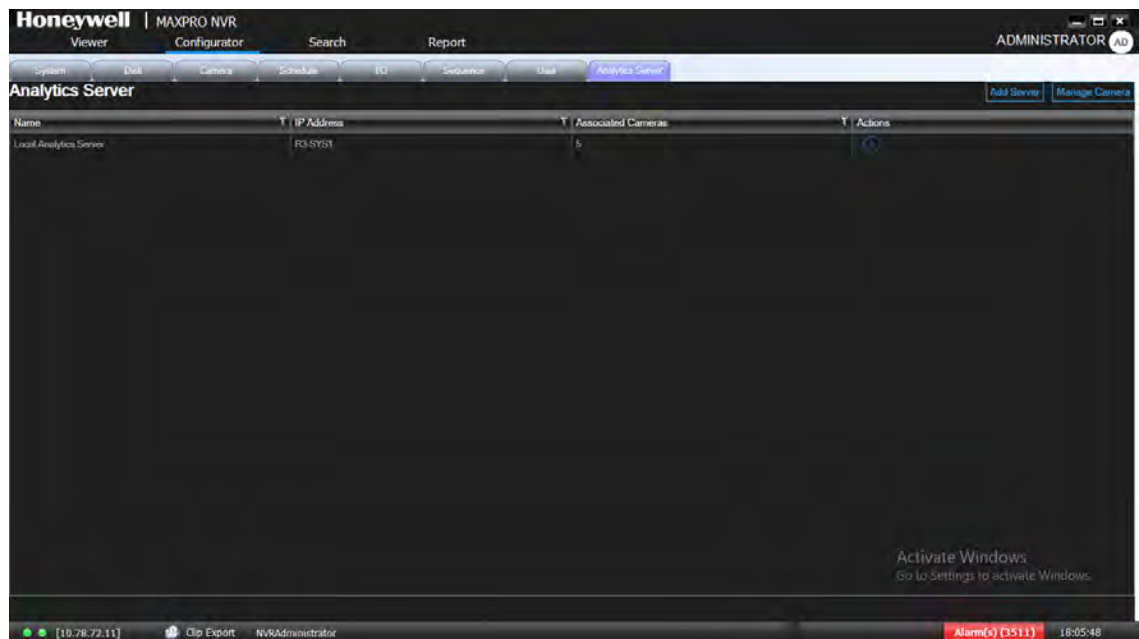
1. In Remote NVR machine, navigate to NVR Bin folder and locate MaproNvrAnalyticServerConfigUtility.
2. Run the Utility in Administrator mode. The Analytics Server Configuration dialog box appears.



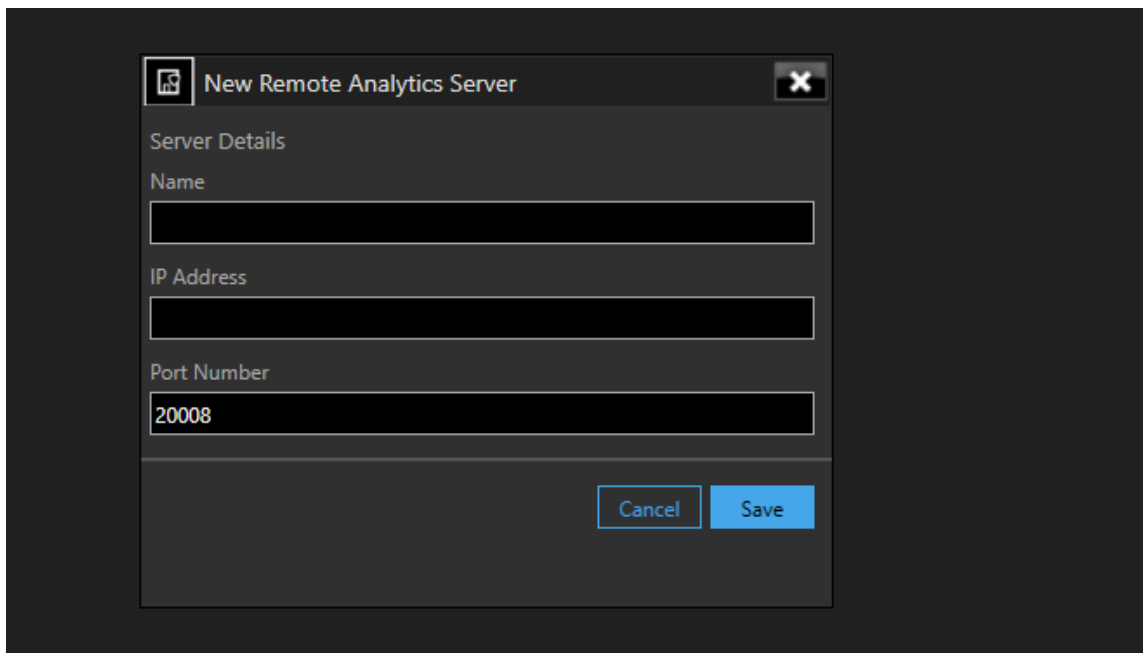
3. Click the “Use as Analytics Server” toggle button to enable.
4. Click the Certificate Setting tab.
5. Under Application Security, click the Certificate Based Encryption option.
6. Type the following details as explained below:
 - Certificate File Path: Browse to select the certificate.
 - Certificate Password: Type the certificate Password
 - Certificate Store Name: Type the certificate Store Name
 - Certificate Subject Name: Type the certificate subject name
7. Click Import Certificate button.
8. Click Save to complete the configuration.

How to Add Analytics Server in NVR Machine

1. In the Configurator > Camera tab, click the Analytics Server tab. The Analytics Server screen is displayed with the list of analytics server already configured.



2. Click Add Server from the right most corner of the screen.

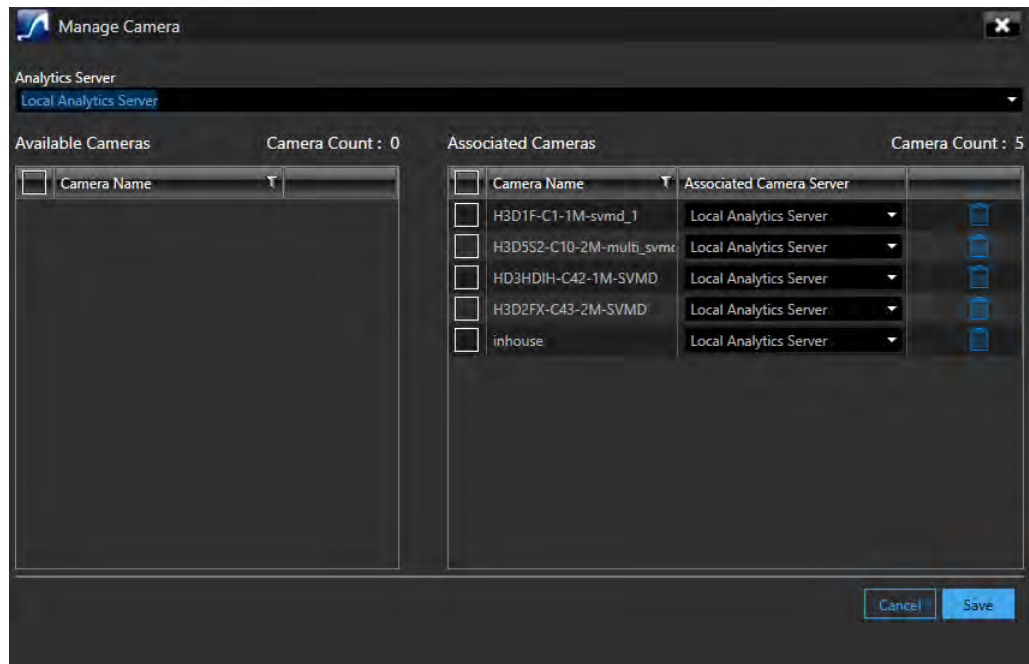


3. For the New Remote Analytics Server provide Server Name, IP Address and Port Number of the server.
4. Click Save to add the new analytics server.

Manging Cameras for Analytics Server

This window allows you to assign analytics server to multiple cameras in bulk. If you have multiple analytics server then you can associate specific cameras to view the alarms accordingly.


1. In the Analytics Server screen, click Manage Cameras from the right most corner of the screen. The Manage Camera dialog box is displayed.

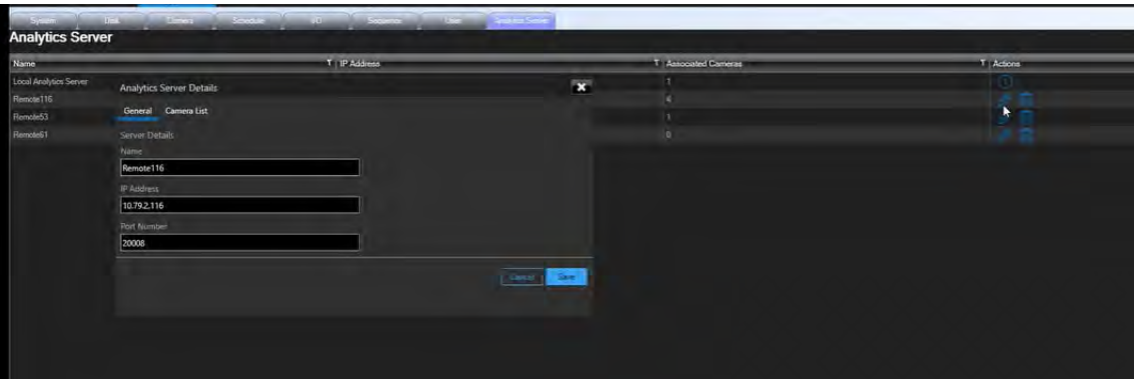


2. From the Analytics Server drop-down, select the required server. This selection applies to all the cameras that will be associated in next steps.
3. From the Available Cameras pane, select the required camera check boxes to associate
4. Click Save. The selected cameras are displayed in Associated Cameras pane.

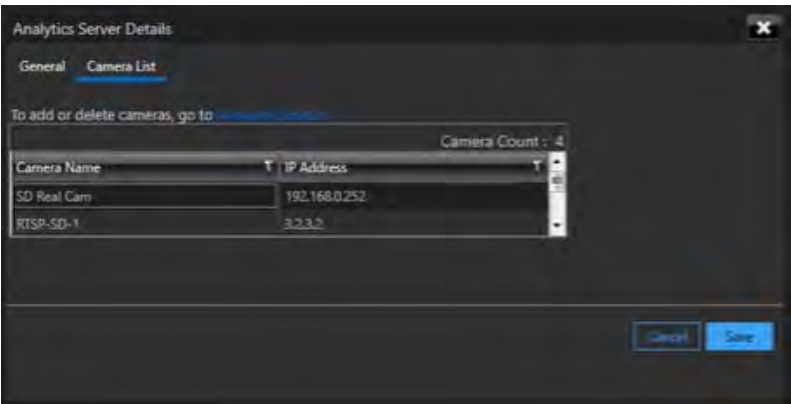
Note: If you want to assign a different analytic server to a specific camera, then under Associated Cameras > Associated Camera Server, select the required server from the drop down list.

Editing Remote Analytics Server Details

1. In the list of Analytics Server, click . The Analytics Server Details box is displayed. By default General tab is displayed.



2. Under Server Details, edit the Name, IP Address and Port number of the NVR machine.
3. Click Camera tab to view the list of cameras associated.



4. To add or delete the associated cameras, then click the Manage Camera link to view the Manage Camera dialog box, See [Managing Cameras for Analytics Server](#) section.
5. Click Save.

Bulk configurations of cameras from NVR

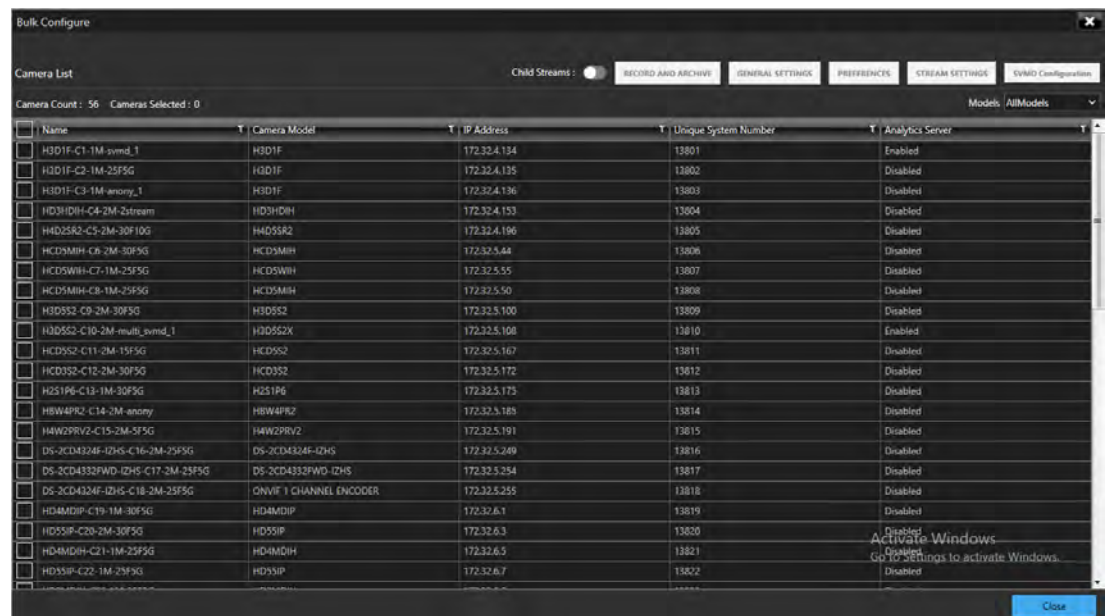
This feature allows you to perform Bulk camera configuration for main and sub stream's, to ease the effort of configuring multiple cameras at the customer site. This feature improves the productivity for dealers and system integrators while configuring many NVRs. The configuration of cameras from the NVR is done one by one today (either post discovery or manual addition). This leads to higher lead time to configure and setup customer sites. Refer to the MAXPRO VMS R670 Installation and Configuration Guide on how to configure and use this feature.

You can perform the following using Bulk configuration screen:

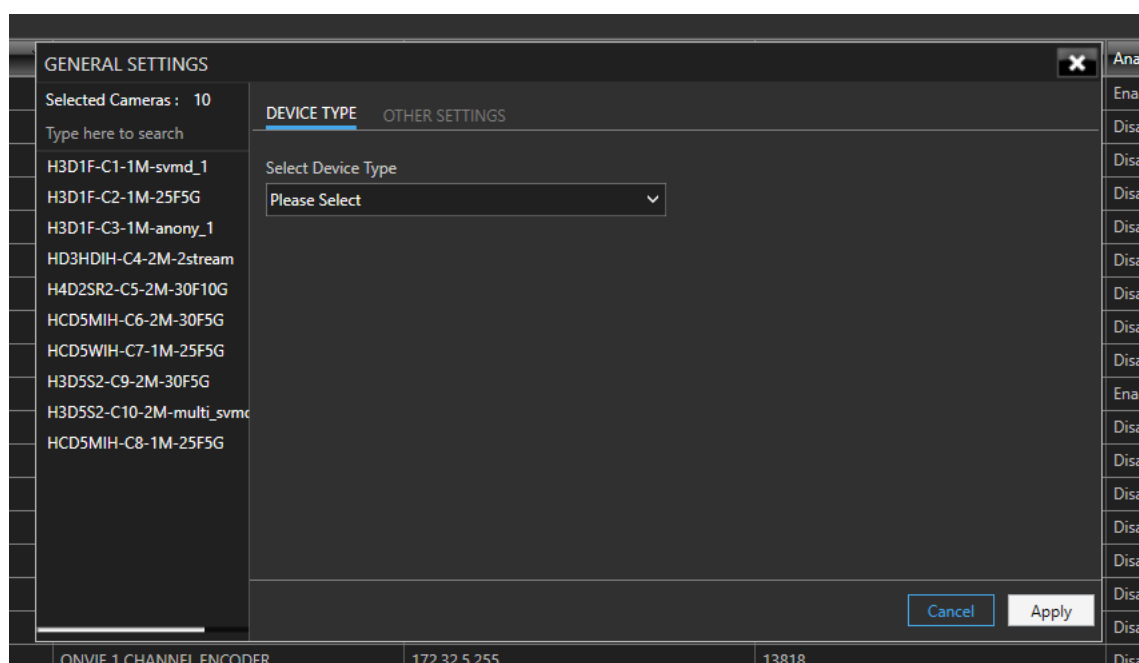
- General Settings
- Record and Archive Settings
- Preference Settings
- Stream Settings including child stream configurations specific to camera model
- SVMD Configuration

How to configure General Settings for cameras in bulk

1. In the camera tab, click Bulk Configure button at the bottom of the screen. The Bulk Configure screen is displayed.

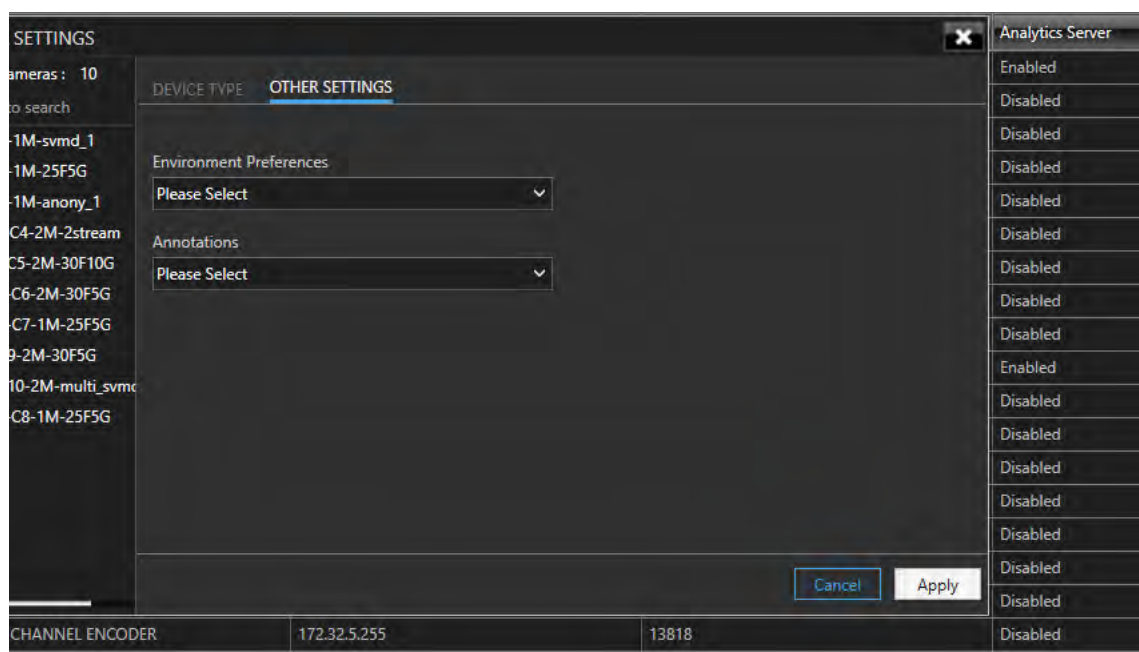


2. Select the required number of camera check boxes and then click the General Setting button. The General Setting dialog box is displayed.



Note: The Stream Settings and Preferences buttons will be enabled while configuring Child Streams. User need to enable Child Streams toggle button to configure streams.

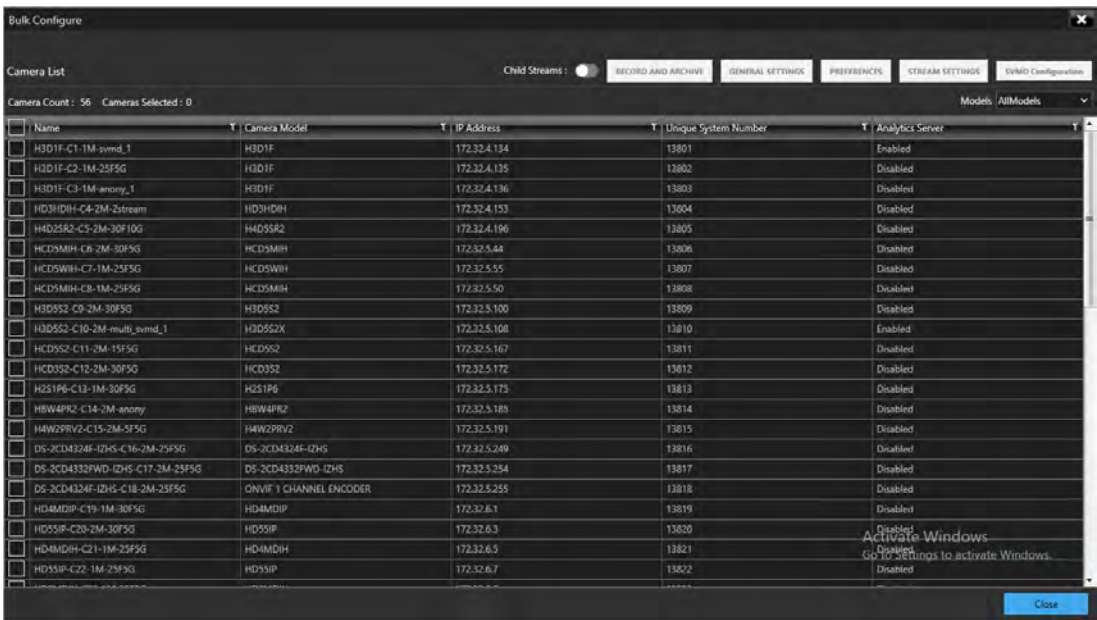
3. In Devices Type tab, select the Device Type from the drop down list.
4. Click Other Settings tab, select Environment Preferences and Annotations options from the drop-down list.



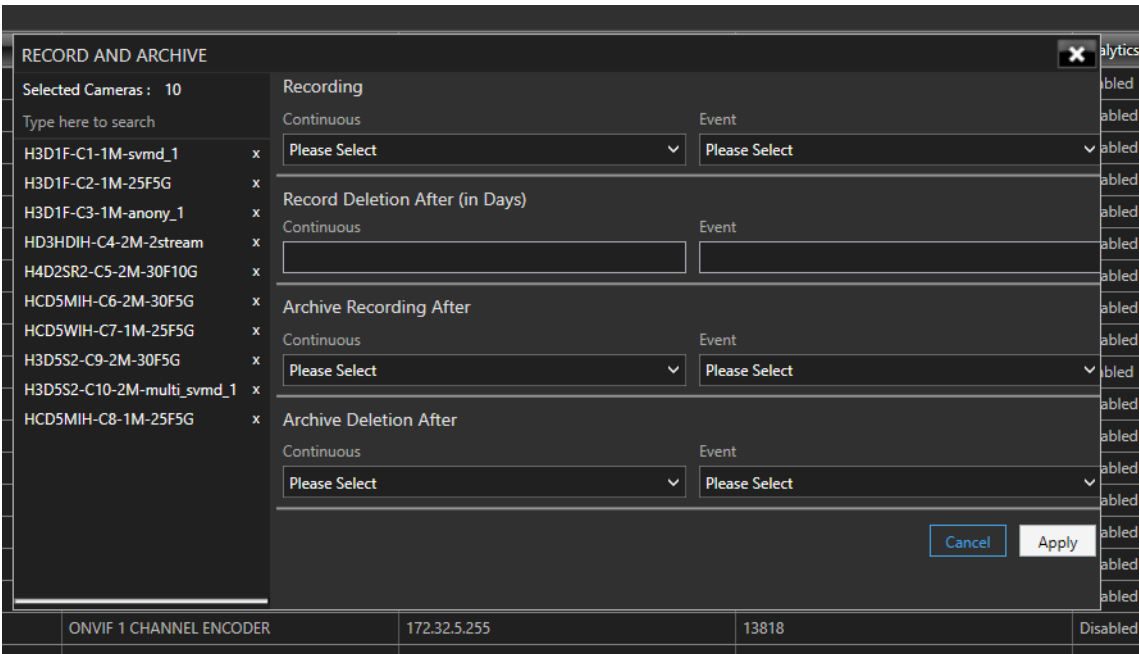
5. Click Apply to complete general settings fro the selected cameras.

How to configure Record and Archive Settings for cameras in Bulk

1. Navigate to the Bulk Configure screen.



2. Select the required number of camera check boxes and then click the Record and Archive button. The Record and Archive dialog box is displayed.



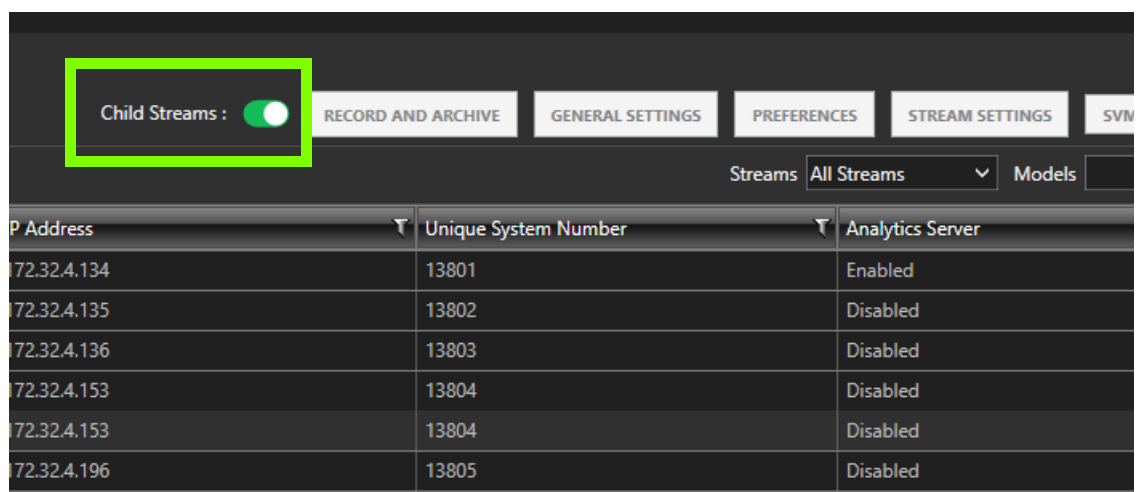
3. On Selected camera pane, the list of selected camera are displayed. You can also search and add more cameras or remove the cameras from here.

4. Select and enter the following as explained below:
 - Continuous - Select the FPS for Continuous recording.
 - Event - Select the FPS for Event based recording.
 - Recording Deletion 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.
5. Click Apply to complete the configuration.

How to configure Preferences for cameras in Bulk

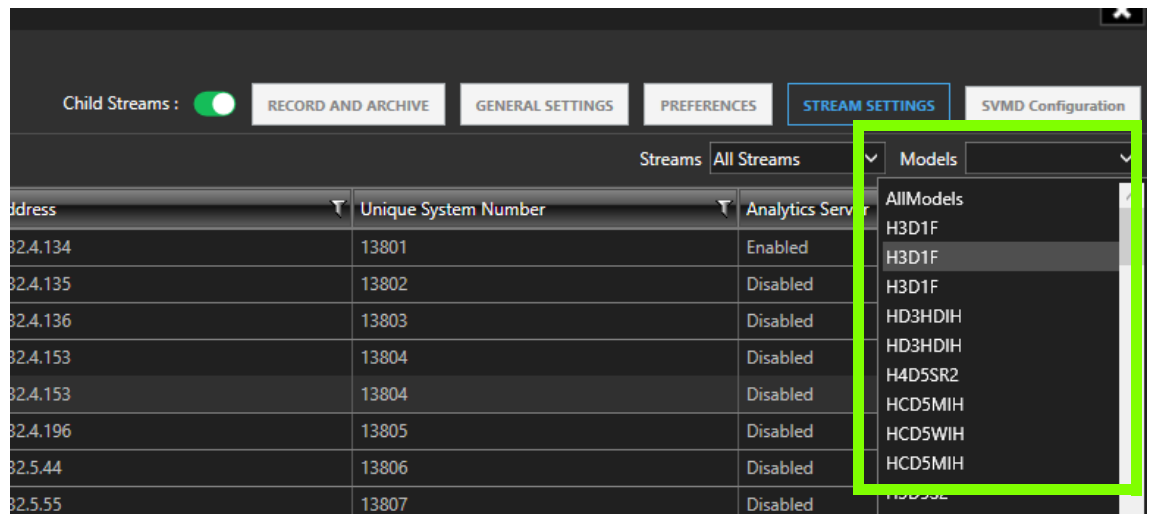
Note: Preferences setting is applicable only to the specific camera models. User need to select the camera models which supports multi streams.

1. Navigate to the Bulk Configure screen and then enable the Child Streams toggle button as shown below.

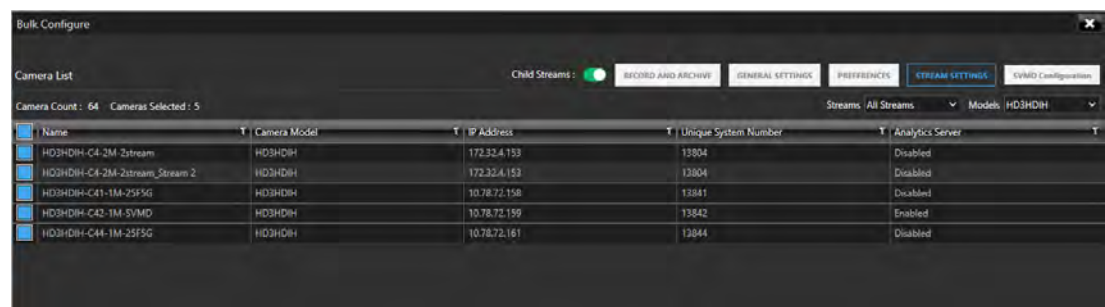


2. Select the required cameras of same model.
Or
Select the required model of camera from the Model drop-down list as shown below.

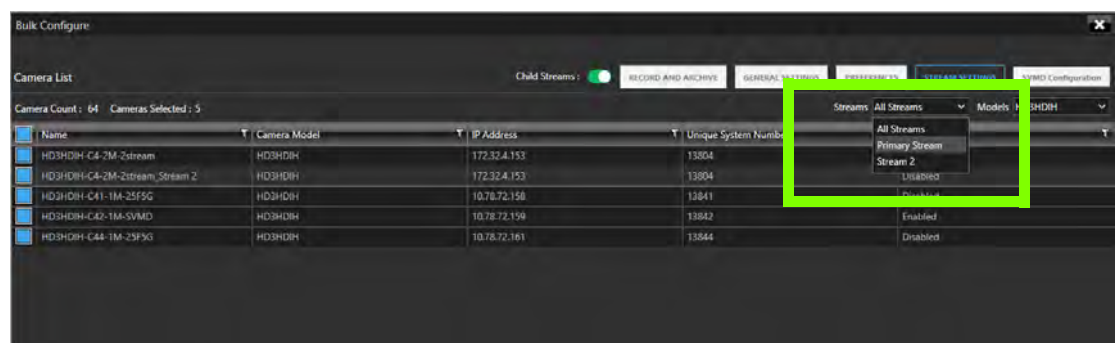
Note: If cameras with different models are selected then a message, Stream of same model should be selected is displayed at the bottom of the screen. Click OK to proceed.



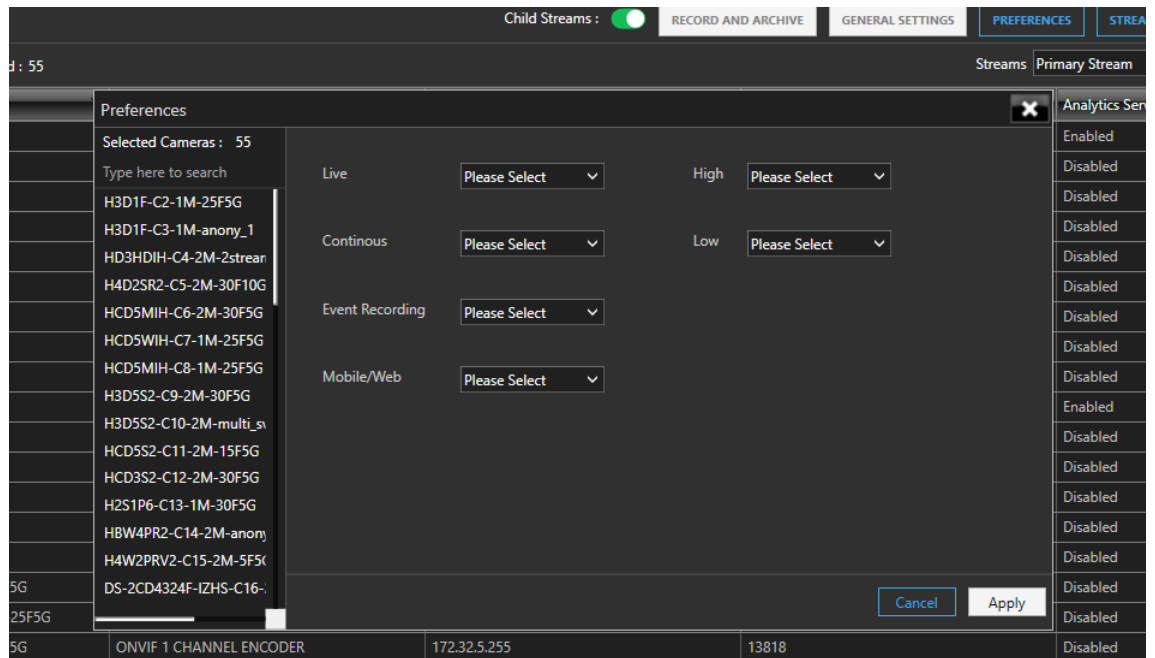
The selected models are displayed as shown below:



3. Select the required Stream from the drop-down list



4. Click the Preferences button. The Preferences dialog box is displayed.

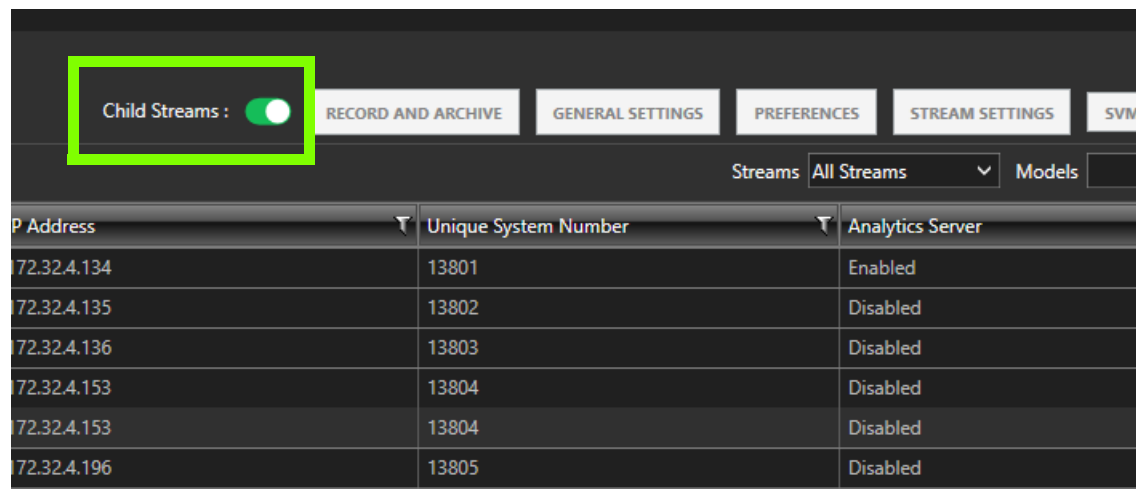


5. On Selected camera pane, the list of selected camera are displayed. You can also search and add more cameras or remove the cameras from here
6. Perform the following as explained below:
 - Live - Select the preferred stream of the camera which you want to use for streaming live video.
 - Continuous - Select the preferred stream of the camera which you want to record continuously.
 - Event Recording - Select the preferred stream of the camera which you want to record on events.
 - Mobile/Web - Select the preferred stream of the camera which you want to use for streaming in Mobile/Web application.
 - High - Select the preferred stream of the camera which you want to categorize as High Resolution stream.
 - Low - Select the preferred stream of the camera which you want to categorize as Low Resolution stream.
 - Click Apply to complete the configuration

How to configure Stream Settings for cameras in Bulk

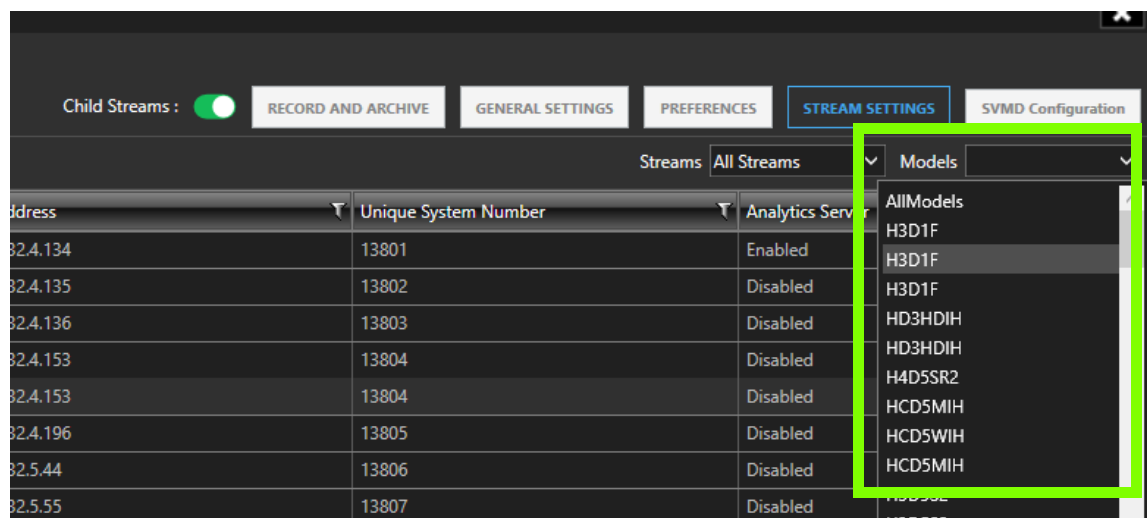
Note: Stream setting is applicable only to the specific camera models. User need to select the camera models which supports multi streams.

1. Navigate to the Bulk Configure screen and then enable the Child Streams toggle button as shown below.



2. Select the required cameras of same model.
Or
Select the required model of camera from the Model drop-down list as shown below.

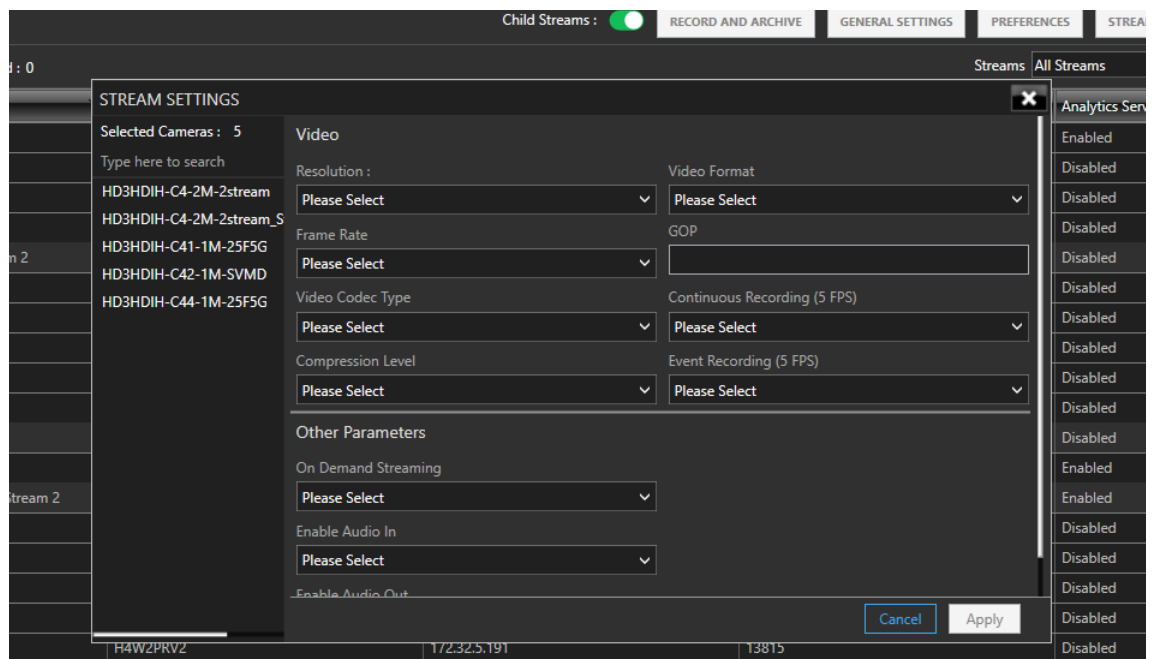
Note: If cameras with different models are selected then a message, Stream of same model should be selected is displayed at the bottom of the screen. Click OK to proceed.



The selected models are displayed as shown below:



3. Click the Stream Setting button. The Stream Setting dialog box is displayed.

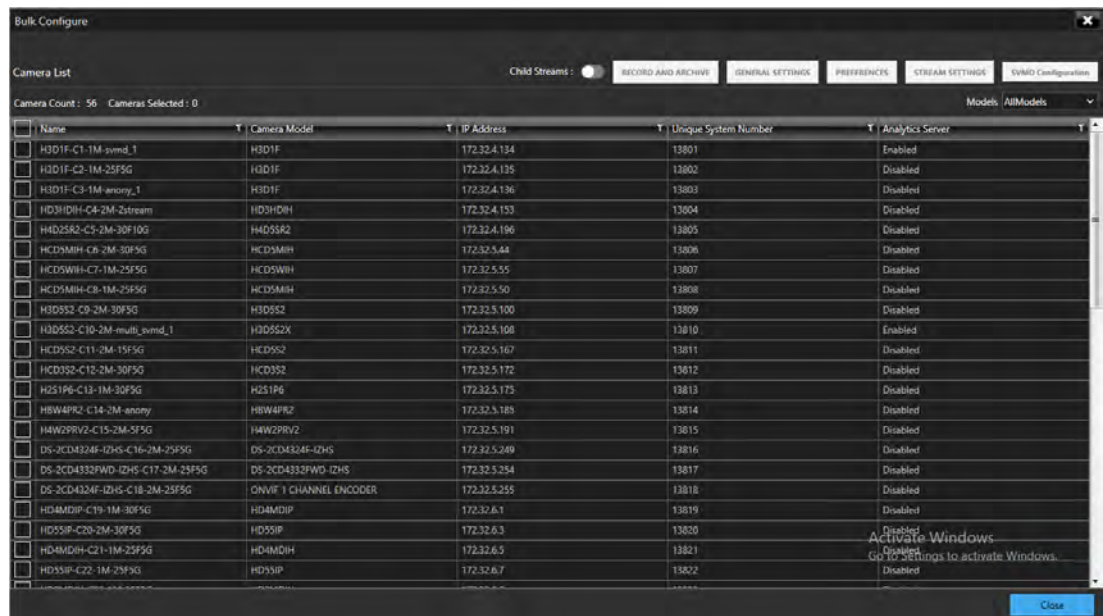


- On Selected camera pane, the list of selected camera are displayed. You can also search and add more cameras or remove the cameras from here
- Under Video configure the following as explained below:
 - Resolution - The Resolution is defaulted to a fixed value based on the camera model (for example, 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.
 - 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.

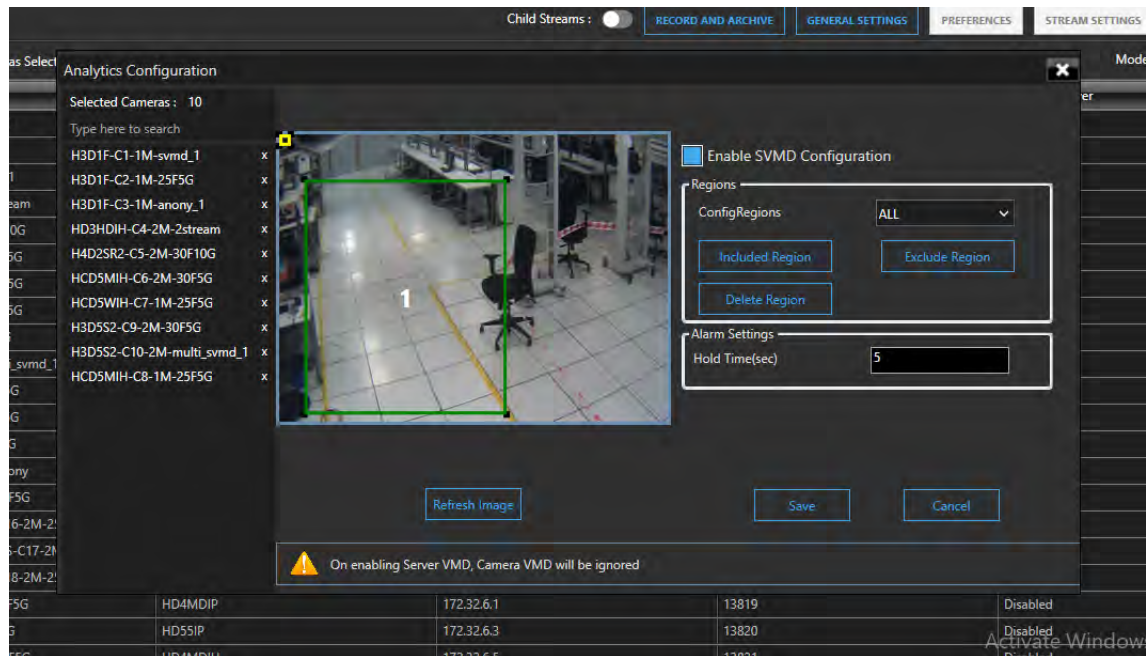
- Compression Level - The Compression Level is defaulted to “Medium”. You can select a new Compression ratio as applicable.
 - Video Format - Select the Video Format (NTSC or PAL). The NTSC and PAL are the widely used video formats.
 - GOP - The GOP is defaulted to “5”. Type a new GOP as applicable. 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.
 - Continuous Recording (5 FPS) - Select the FPS for Continuous recording.
 - Event Recording (5 FPS) - Select the FPS for Event based recording.
 - Under Other Parameters
 - Select the On Demand Streaming options from the drop-down list.
 - Enable Audio In/Out: This is for audio supported camera. Select the required In and Out option from the drop-down list.
6. Click Apply to complete the configuration

How to configure SVMD for cameras in bulk

1. Navigate to the Bulk Configure screen.



2. Select the required number of camera check boxes and then click the SVMD Configuration button. The Analytics Configuration dialog box is displayed.



3. Select the Enable SVMD Configuration check box

Under Regions, click the Include Region button to create required numbers of region(s) on the image.

4. Select the required region to display from the Region drop-down. Available options are All, None or (Region 1, 2, 3 and so on). Configure the Object size threshold if required.

5. If you want to exclude any region then select the region using mouse and then click Exclude Region button.

6. Under Alarm Settings, set the Alarm Hold time in seconds.

7. Click Save to complete the configuration.

Bi-Directional Audio Support for MAXPRO NVR

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

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

Note: Only Honeywell ONVIF Camera models are supported.

Only fixed G.711 ulaw Codec format is supported.

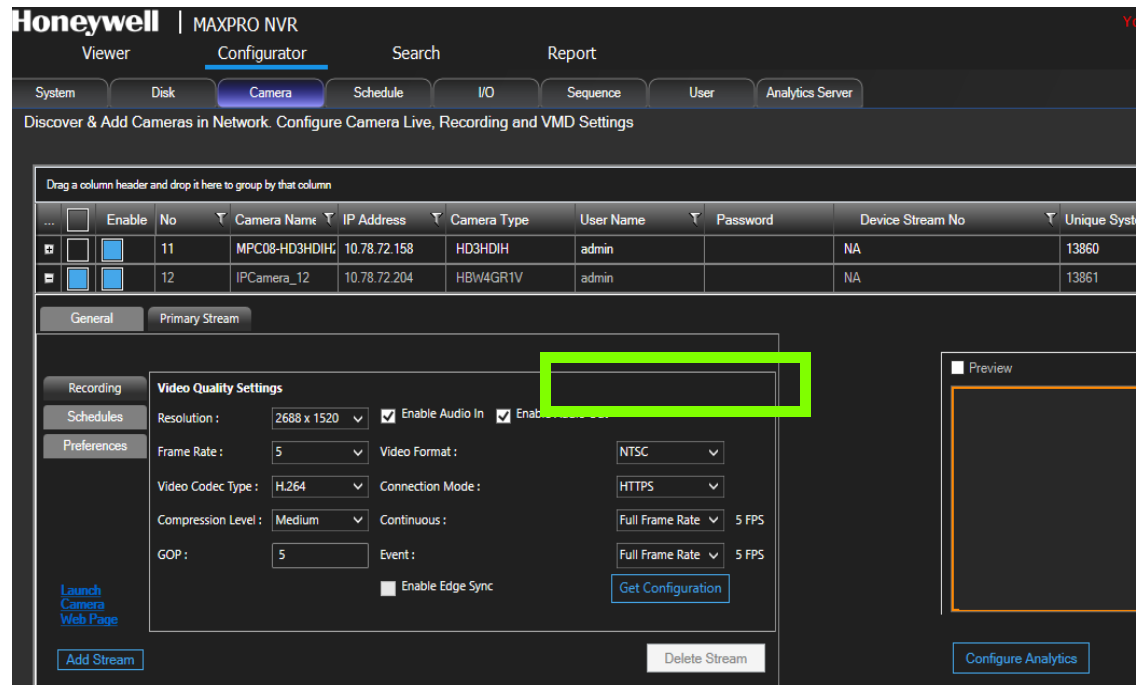
Mutlistream is supported, but can be enabled in only one stream at a time.

It is recommended for the user to enable and speak for one camera at a time.

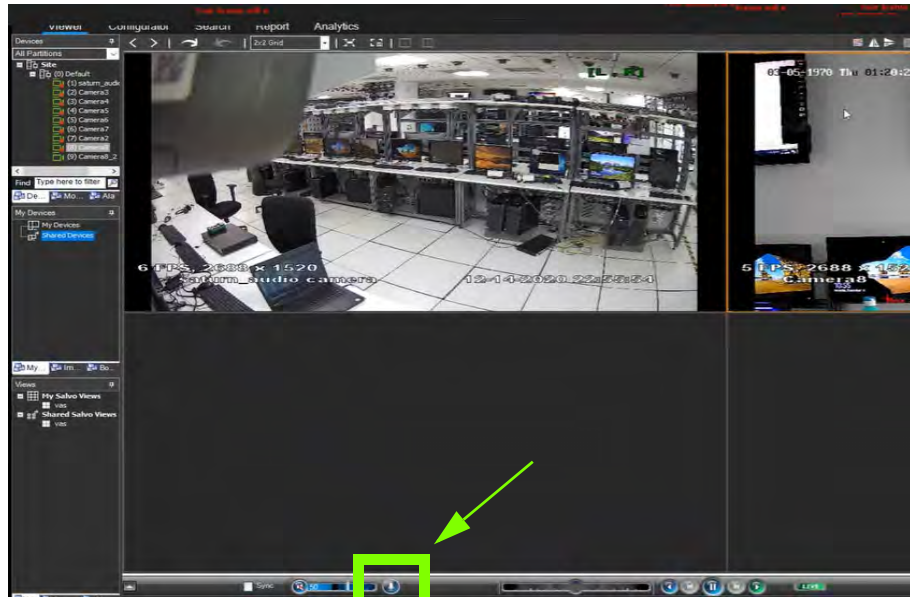
Windows 2016, 2019 windows server machines are not supported for beta release.

How to configure Bi-Directional Audio for a camera

1. In NVR, for a Honeywell Onvif camera, navigate to Camera properties > Primary Stream > Recording tab.



2. For a specific stream, select the Enable Audio In/Out check boxes as explained below:
 - Enable Audio In: Camera to VMS Operator
 - Enable Audio Out: Operator to camera connected with speakers.
3. In VMS > Viewer screen. select the audio enabled camera in the panel (One at a time) and then enable the Mic button on the Timeline bar to speak and Disable the Mic button to end the speech as highlighted below.



Limitation

- AAC compression format is not supported for Audio Out from MAXPRO NVR. It is recommended to configure G711 u law as Audio Out compression format in the camera webpage.
- From NVR to VMS, user will notice a latency of 1.5 Seconds in audio.

Series 60 Camera Integration

MAXPRO VMS R670 supports Series 60 Camera integration with MAXPRO NVR 6.7 recorder. The following tables explain the list of supported camera models and firm-ware details.

Type	Camera Models	Firmware Details
Premium Model	HC60W35R2	Honeywell_L60-Series_IPC_HC60WXXRX_V1.0.21.20200828
	HC60W35R4	
	HC60W45R2	
	HC60W45R4	
	HC60WB5R2	
	HC60WB5R5	
	HC60WZ2E30	
Mainstream Model	HC60W34R2L	
	HC60W34R2	
	HC60W44R2L	
	HC60W44R2	
	HC60WB4R2L	
	HC60WB4R2	

Allgovision Analytics Box Support

Pro-Watch VMS R670 release supports integration with Allgovision analytics that brings real time Facial Recognition (FR) and License Plate Recognition (LPR) alarms into VMS. User can view both FR and LPR related alarms in one screen and perform surveillance operations. This feature requires a valid license. Refer MAXPRO VMS R670 Operator guide on how to search and view the alarms.

Integrating Allgovision Analytics

The process of Integrating Allgovision analytics in Pro-Watch VMS includes the following:

1. In NVR
 - Create a new Admin Account
 - Add in Web Configurator
2. In VMS:
 - Install R670 and Apply license
 - Create an Administrator Account:
 - Configure Web Configurator
 - Adding Event Server in VMS
3. In Allgovision Analytics Machine:
 - Install the Analytics setup packages in a standalone machine.
 - Add VMS Server
 - Connect to VMS
 - Applying License and Enable Analytics on camera.

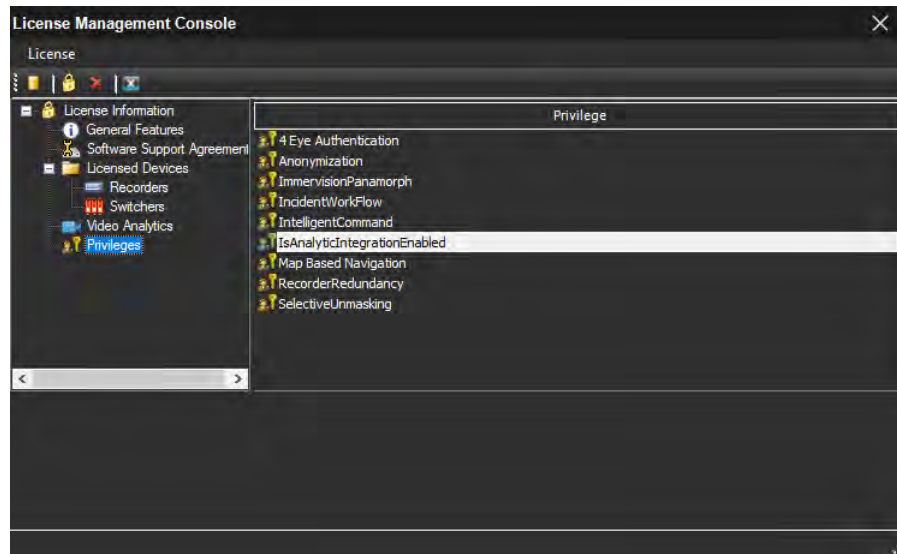
Configurations in NVR

- Create a new Admin Account: Refer to the Pro-Watch NVR 6.7 Installation and Configuration Guide.
- Add in Web Configurator. Refer to the Pro-Watch NVR 6.7 Installation and Configuration Guide on how to add

Configurations in VMS

Install SP1 and Apply license

- See [Upgrade to MAXPRO VMS R670](#) section.
- Apply license and ensure that ISAnalyticIntegrationEnabled entry is displayed in License Management Console Window > Privileges as shown below. Refer to the Pro-Watch NVR 6.7 Operator Guide > Generating and Installing the License for Pro-Watch™ VMS section.



Create an Administrator Account

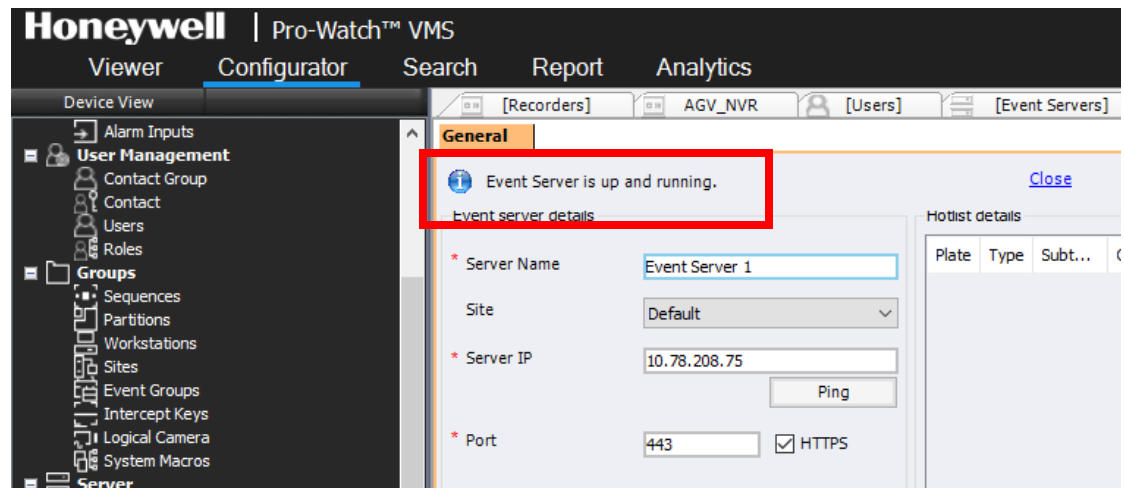
- See [Adding a User](#) section on how to create a user.

Configure the Web Configurator

- Add the newly created administrator account in Web Configurator and then click Save. See [Setting the Pro-Watch™ Web Configurator](#) section for more information.

Add and Configure Event Server

1. Add the Event Server, see [Adding an Analytics Server](#) section.
2. Enter the server IP address and newly created administrator credentials.
3. Ensure that to validate and check whether the Event Server is up and running as shown below.

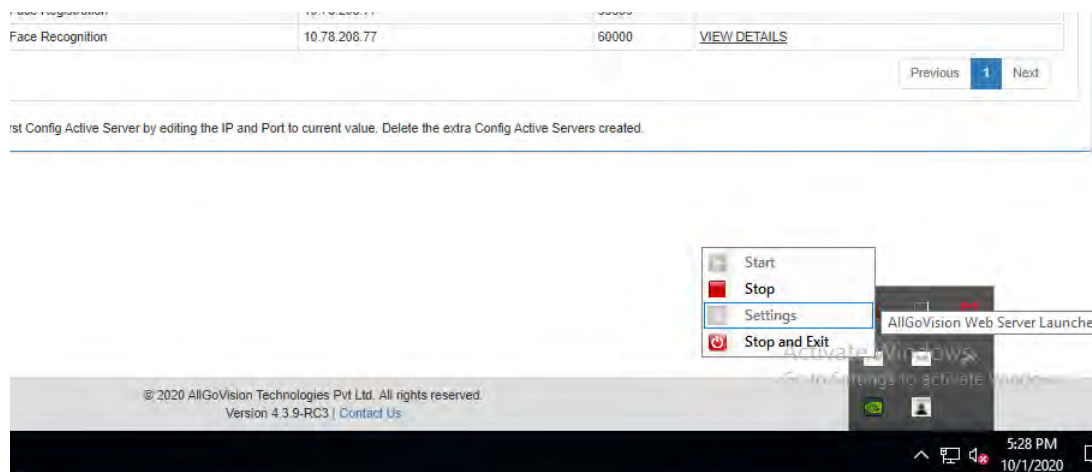


4. Click save

Configurations in Allgovision Analytics Box

Install Allgovision Package

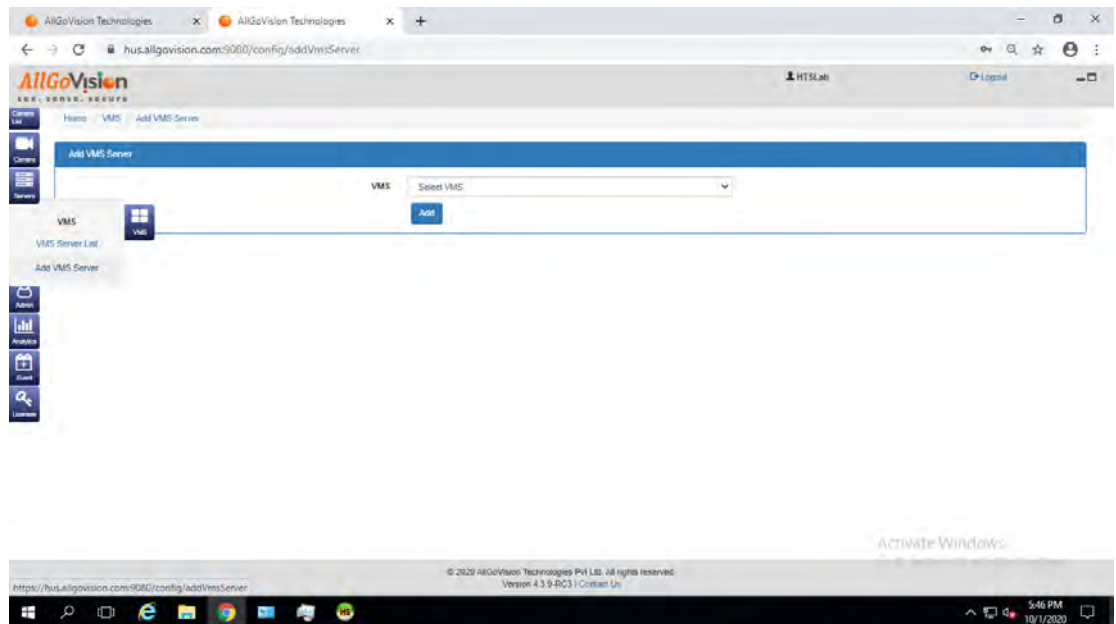
1. Refer to the Allgovision specific documents for more information on how to install the packages.
2. Start the Web Server from system Trey as shown below.



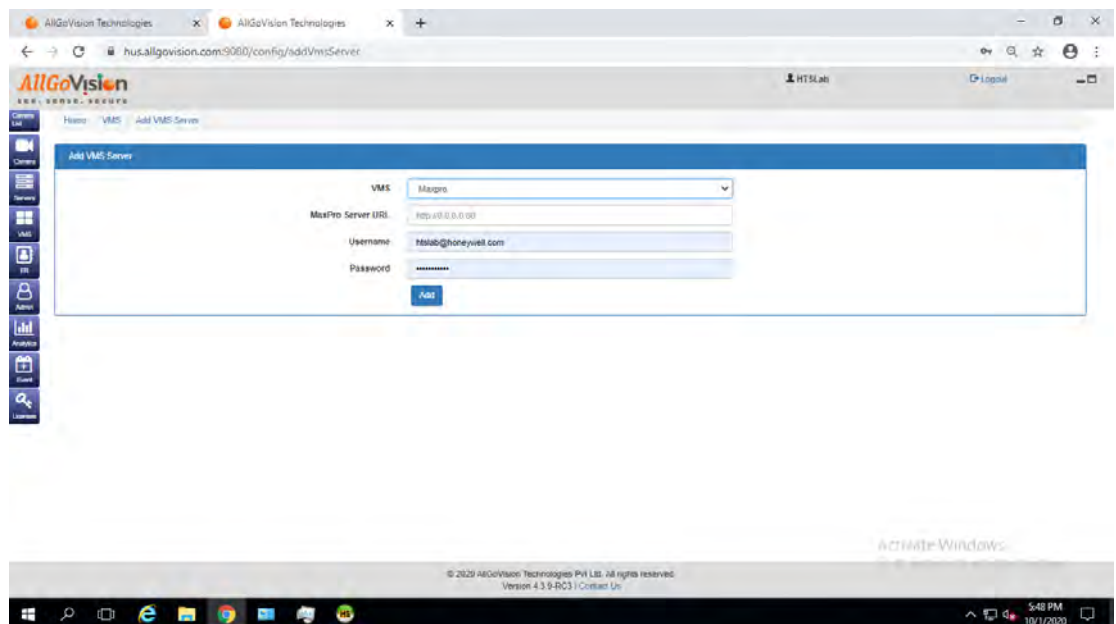
3. Login with credentials created while installing Allgovision packages. Refer Allgovision specific document to login.

Add VMS Server

1. In AllGoVision home page, click VMS tab on the left pane and then click Add VMS Server link as shown below.

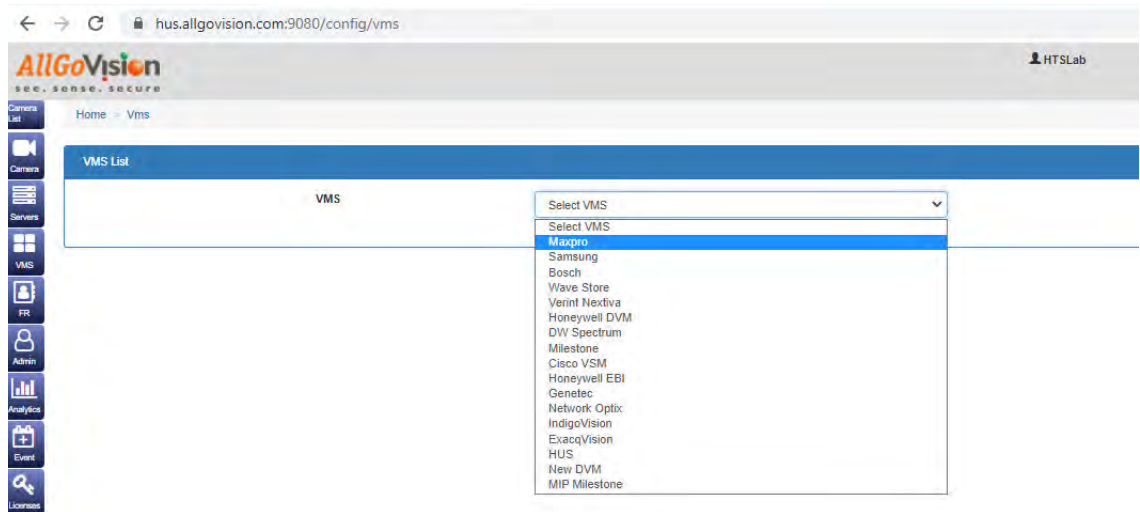


2. From the VMS List, select MAXPRO from the drop down list. The specific parameters are displayed as shown below.



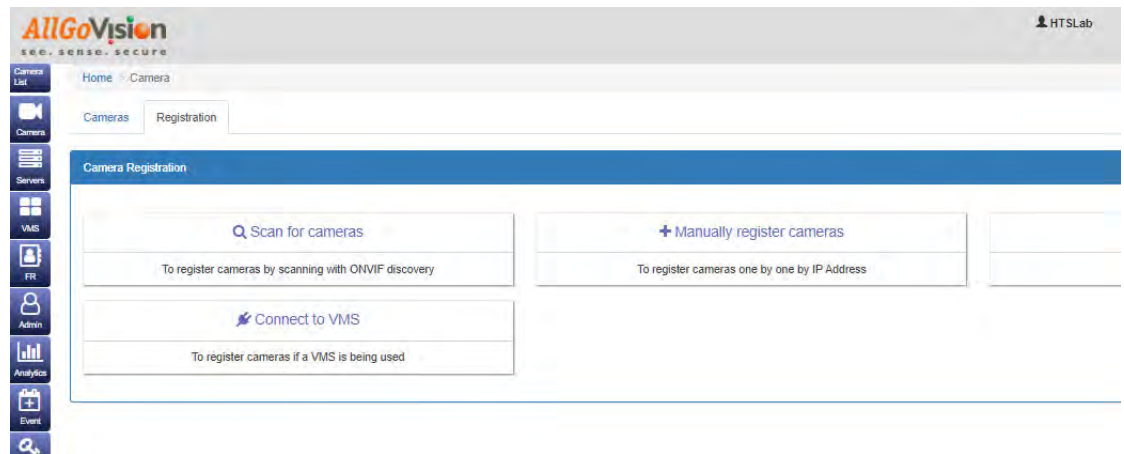
3. Type the MAXPRO VMS Server URL along with IP address in the format `http://<IP Address>`.

4. Type the Username and Password which is created. This should be any administrator username & password of VMS system.
5. Click Add. You can view the newly added VMS Server under VMS tab > VMS Server list as shown below.

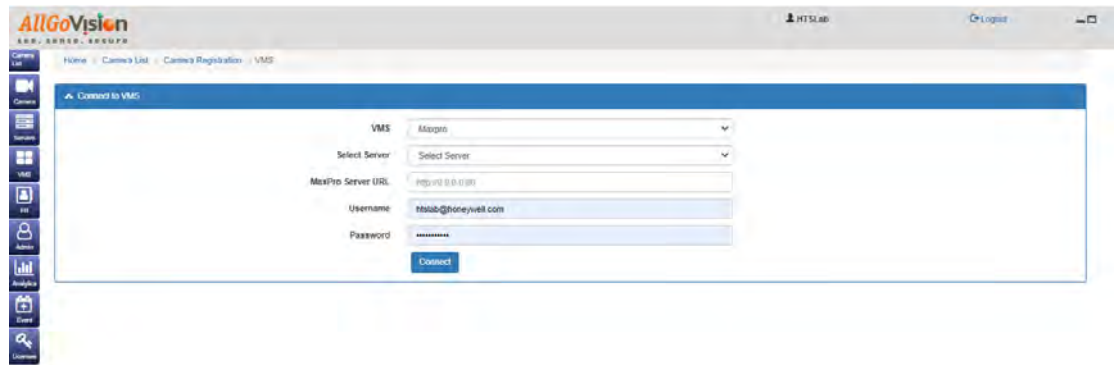


Connect to VMS

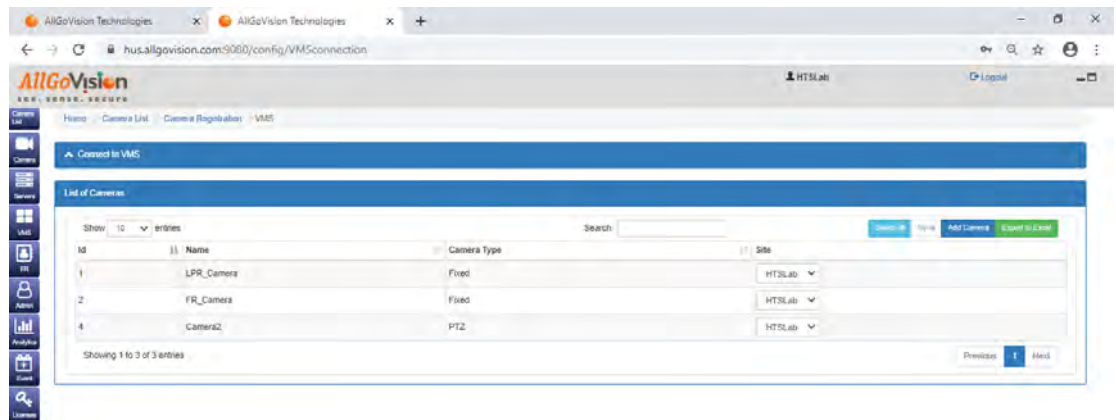
1. On the left pane, click Camera > Register Camera. The Camera Registration page is displayed as shown below.



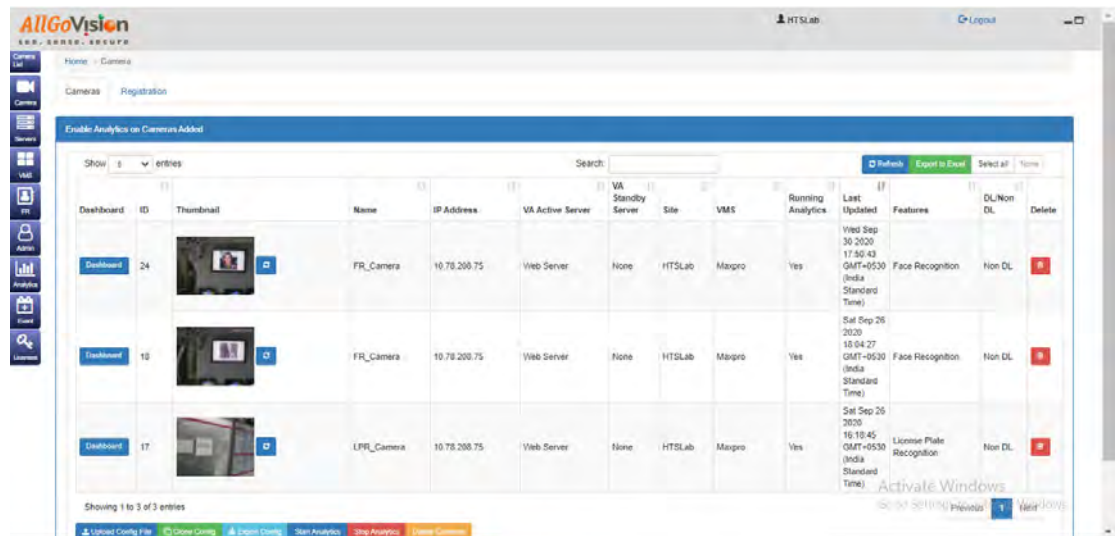
2. Click the Connect to VMS tile. The Connect to VMS page is displayed.
3. From the VMS drop-down list select the VMS which is added. The corresponding parameters are displayed as shown below.



4. From the Select Server drop-down list, select the server IP assigned for VMS. The other fields are updated based on the selection.
5. Click Connect. The List of cameras associated with the VMS is displayed as shown below. Only NVR recorder cameras will be displayed in Allgovision. Third party recorder cameras will not be listed

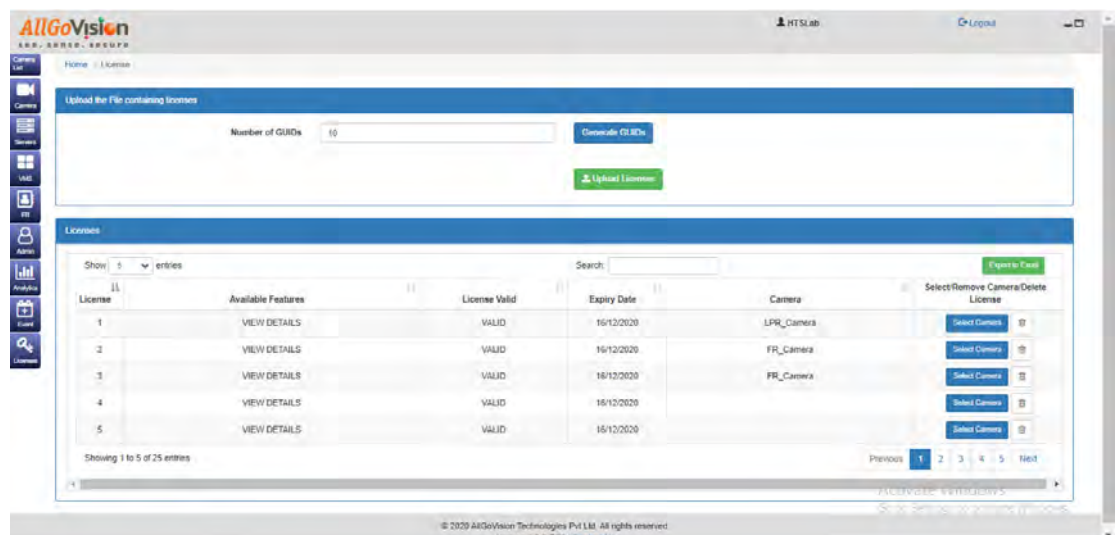


6. Select the required cameras for analytics and then click Add Camera. The selected camera is displayed under Camera list page as shown below.

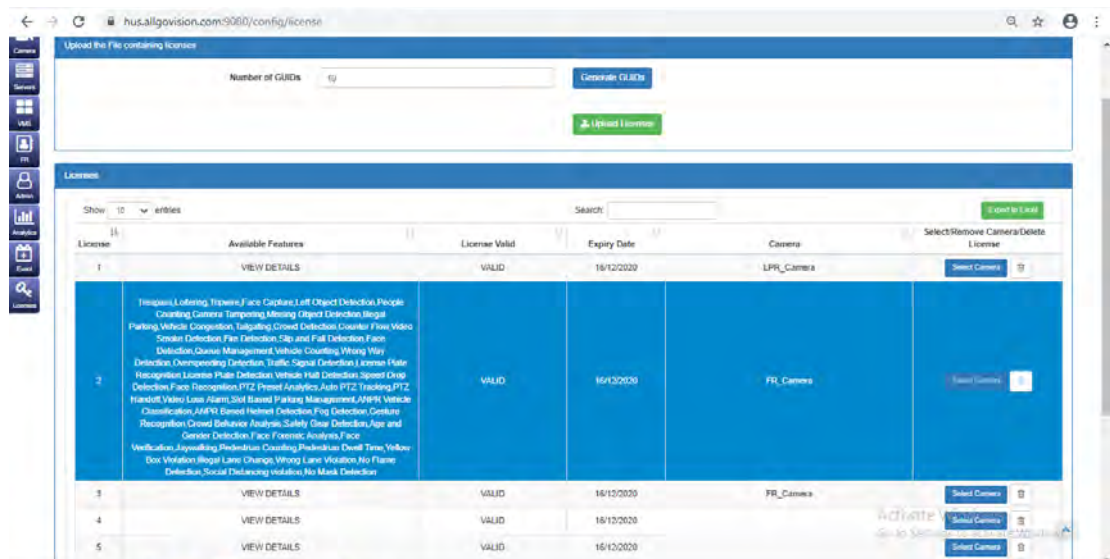


Apply License and Enable Analytics on Cameras

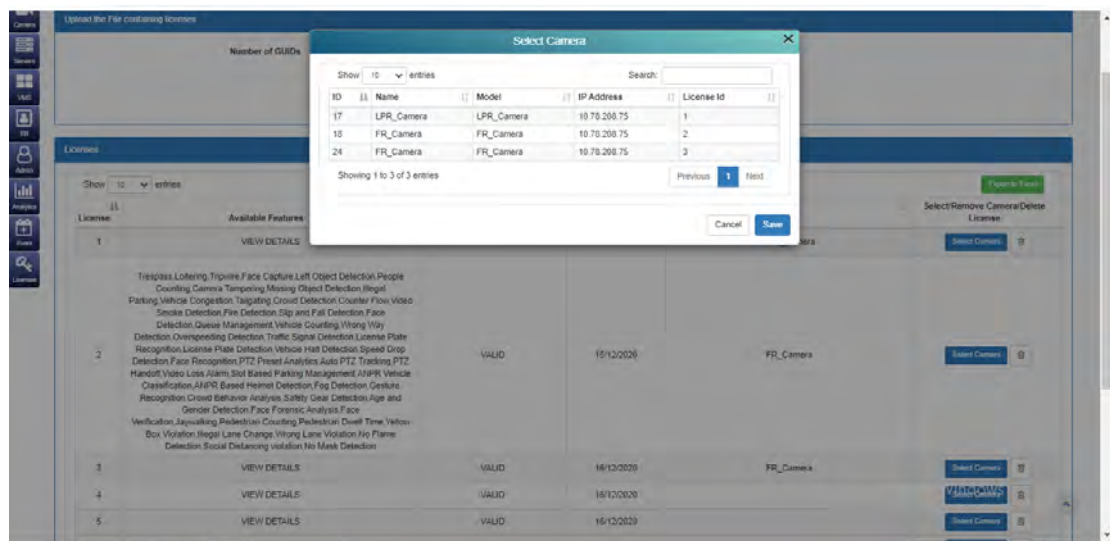
1. Navigate to License tab and then click license Management link. The Licenses page is displayed as shown below.



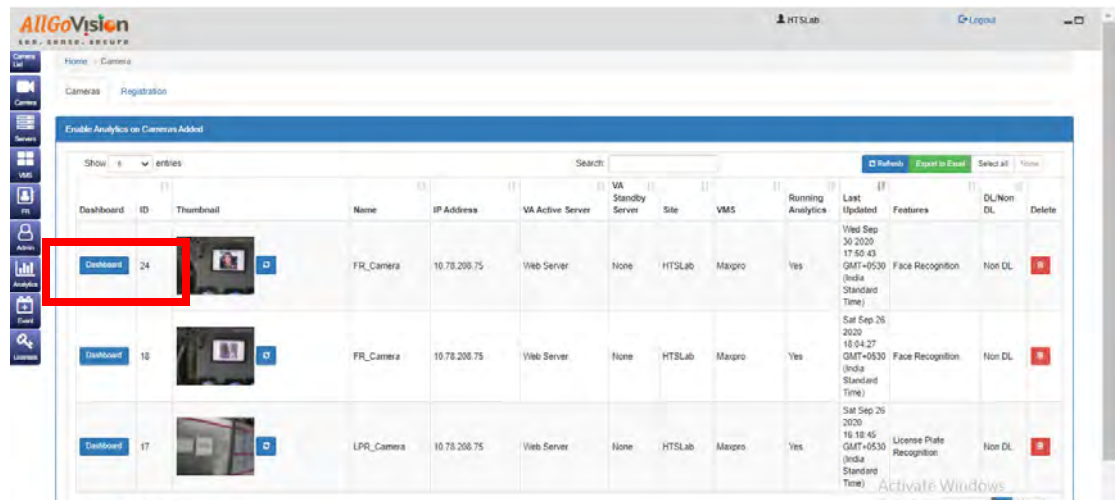
2. In Number of GUIDs box, type the number of cameras for which the analytics license is required.
3. Click Genrate GUIDs to generate a file. This file needs to sent to AllgoVision Support team. The AllgoVision team will provide the licenses in a specific format.
4. Click Upload License button to upload the file received from AllgoVision support team. The license will be provided for the number fo camera.
5. Under Licenses, click on the required camera from the list. The camera details are displayed as shown below.



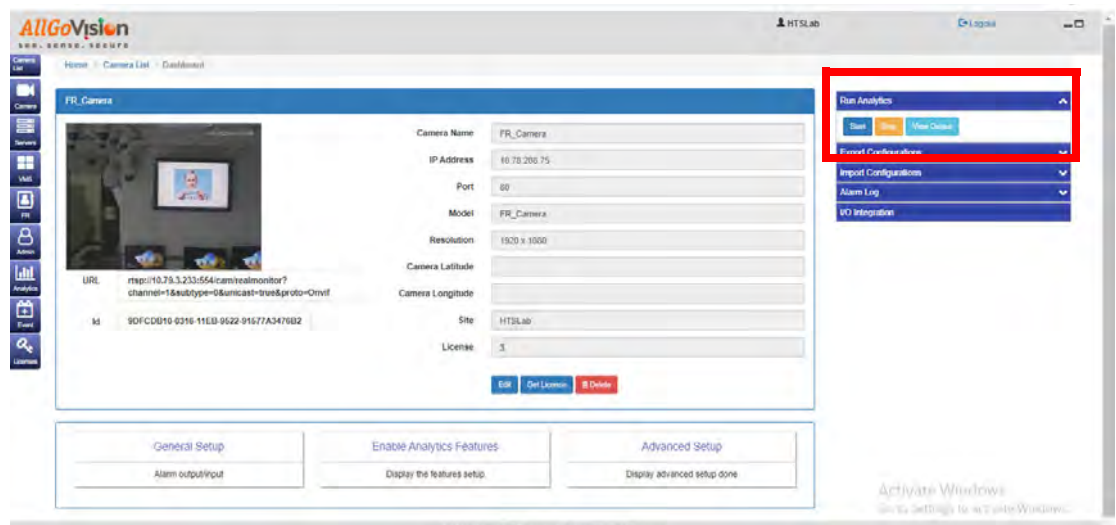
6. Click the Select Camera button. The Select Camera dialog box is displayed as shown below.



7. Select the required camera from the list and then click Save. The license for specific camera will be applied.
8. Navigate to Camera list tab and then click Dashboard button for the specific camera to setup the camera with more options. Refer to the AllgoVision specific documents for more information.



- Once the basic settings are completed, on the right page, expand Run Analytics node and then click to Start button to enable analytics on the camera as shown below.



IDEMIA Integration with MAXPRO VMS

How to configure Idemia with VMS

The following steps describes the configurations needed in Augmented Vision (AV) to integrate with MAXPRO VMS.

Prerequisite

Before starting ensure you perform the following:

- Add a file entry into the VMS Collection of the AV database. This file will contain all the information needed to connect to the Honeywell VMS to send an API call.

The database file gets created into the database when the python script is executed with the VMS parameters. You need to obtain the following AV and VMS information before you can continue:

Parameters	Example: Description
AV Server IP-address	192.168.1.206
VMS IP-address	192.168.1.225
VMS-API login name	testadmin
VMS-API password	Trinity@12345

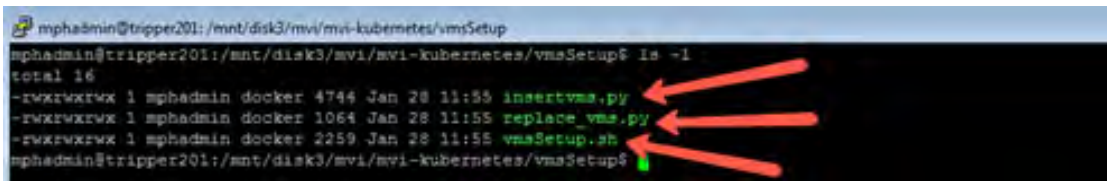
Step 1:

1. Make use of a Linux terminal connection using the AV console or a remote connected Putty session.
2. Login as "mphadmin" and use the password: "Secret+++++++(There are nine plus symbols).

Step 2:

- Run the following in Command prompt window:
- mphadmin@tripper201:~\$ **cd /mnt/disk3/mvi/mvi-kubernetes/vmsSetup**
- mphadmin@tripper201:/mnt/disk3/mvi/mvi-kubernetes/vmsSetup\$ **ls -l**

The following files must be listed to continue:



Step 3:

1. Type in the following command to start the configuration process:
 The sample execution command looks like : `./vmsSetup.sh <vmsUsername> <vmsPassword> <mongo_ip> <vms_ip>`

<vmsUsername> : The username of the VMS Camera.
 <vmsPassword> : The password for the VMS Camera.
 <mongo_ip> : The IP of the Mongo machine.
 <vms_ip> : The IP of the VMS Camera.

For help before executing the script, you can run the following command: `./vmsSetup.sh -h`.

The following response is displayed as shown below:

```
mphadmin@friday:/mnt/disk3/vms$ ./vmsSetup.sh -h
[INFO]: This script is to perform the VMS Setup on AV deployed system.

[INFO]: This script needs some parameters for execution
Syntax: vmsSetup.sh <vmsUsername> <vmsPassword> <mongo_ip> <vms_ip>

Parameters:
vmsUsername      The username for the VMS Camera.
vmsPassword      The password for the VMS Camera.
mongo_ip         Ip of the mongo machine.
vms_ip           Ip of the VMS Camera.
```

The sample execution command looks like:

./vmsSetup.sh testadmin Trinity@12345 192.168.1.206 192.168.1.225

Expected Response: “Document Insertion Success”

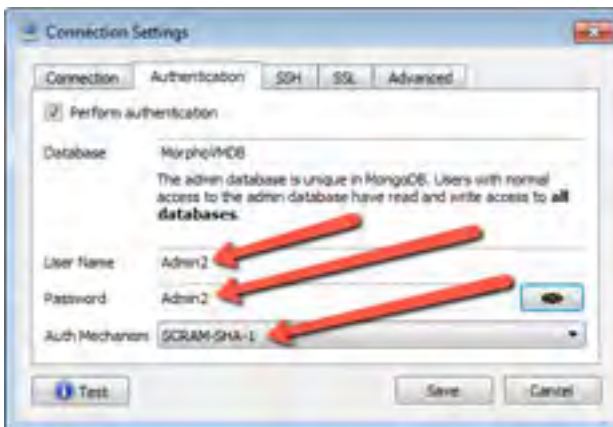
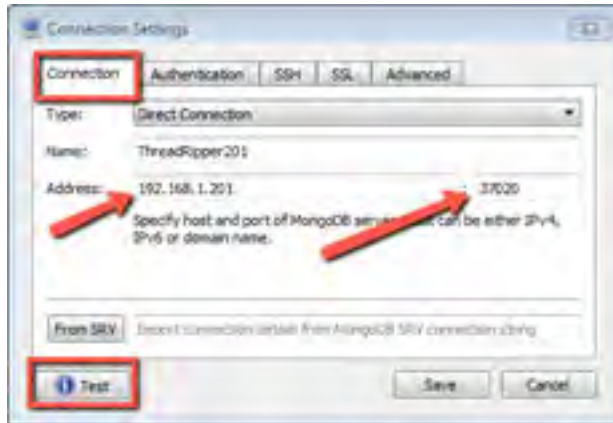
After execution you can see the following messages on the console window:

```
mphadmin@friday:/mnt/disk3/vms$ ./vmsSetup.sh testadmin Trinity@12345 192.168.1.206 192.168.1.225
[INFO]: Replacing the values of VMS Username and Password in config_stability.sh
[INFO]: Executing copy_conf.sh.
cp -r ./vms-share/grafana /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/jboss-config /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/jboss-roles-user /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/license-server /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/hdfs-config /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/vault /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/idevsa-vault /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/testide /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/certificates /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/reports /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/mbs-cert /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/ccturn /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/kuowento /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/hashicorp-vault /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/mediamanager /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/cave-import /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/ondemandreport /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/ock /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/mongodb-keyfile /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
cp -r ./vms-share/mongodb-data /var/lib/docker/disk3/mvi_dev/dev3/mvi-share/
[INFO]: Restarting the hashicorp_vault pod.
configmap "key-mapper" deleted
deployment.extensions "mvishashicorpvault" deleted
service "mvishashicorpvault" deleted
configmap/key-mapper created
deployment.extensions/mvishashicorpvault created
service/mvishashicorpvault created
[INFO]: Adding VMS Camera details as document in the VMS Collection in 192.168.1.206 MongoDB.
[INFO]: connecting to MongoDB...
[INFO]: Deleting existing record of MAXPRO
[INFO]: Document Insertion Success.
```

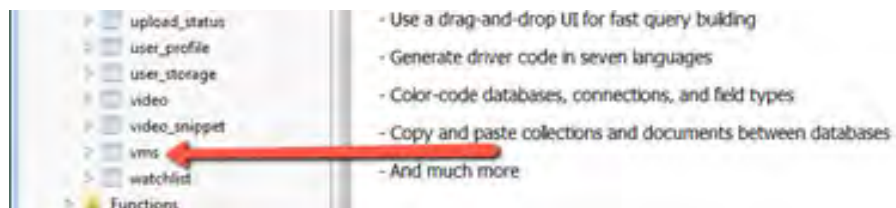
Step 4:

To ensure the information in the database is correct, use the Robo3T application and view the VMS entry. Ensure that the AV and VMS information is accurate. Use the login credentials as shown below:

- IP Address: 192.168.1.206 (this is only an example IP), Port: 37020
- Username: Admin2, Password: Admin2



2. Connect to the database.
3. Under the Collections tab, open the vms file. Ensure the following entries are created.





```
db.getCollection('vms').find({})
[{"_id": "ObjectId('5fa2bc92c46ed009b4d1405')",
  "config": {
    "send_notifications": "true",
    "user": "testadmin",
    "port": 80,
    "pw": "Trinity91143",
    "uri": "http://192.168.1.225/VSICM/ICM/DeviceGet/Camera(0)/FullEntityToAllStar(CameraAssignToPNIPData)Id93D(conf)",
    "modelName": "model",
    "send_alarm": "true",
    "notification_url": "https://192.168.1.225/metadata/ICM/EventMgmt/EventStreams/3022/outputFormat=Geometry",
    "playback": {
      "file_service_url": ""
    }
  },
  "notificationLikelihoodPercent": 88/100,
  "alarmLikelihoodPercent": 94/100,
  "type": "VMS_CAMERA",
  "name": "Honeywell Margro VMS"
}]
```

Step 5:

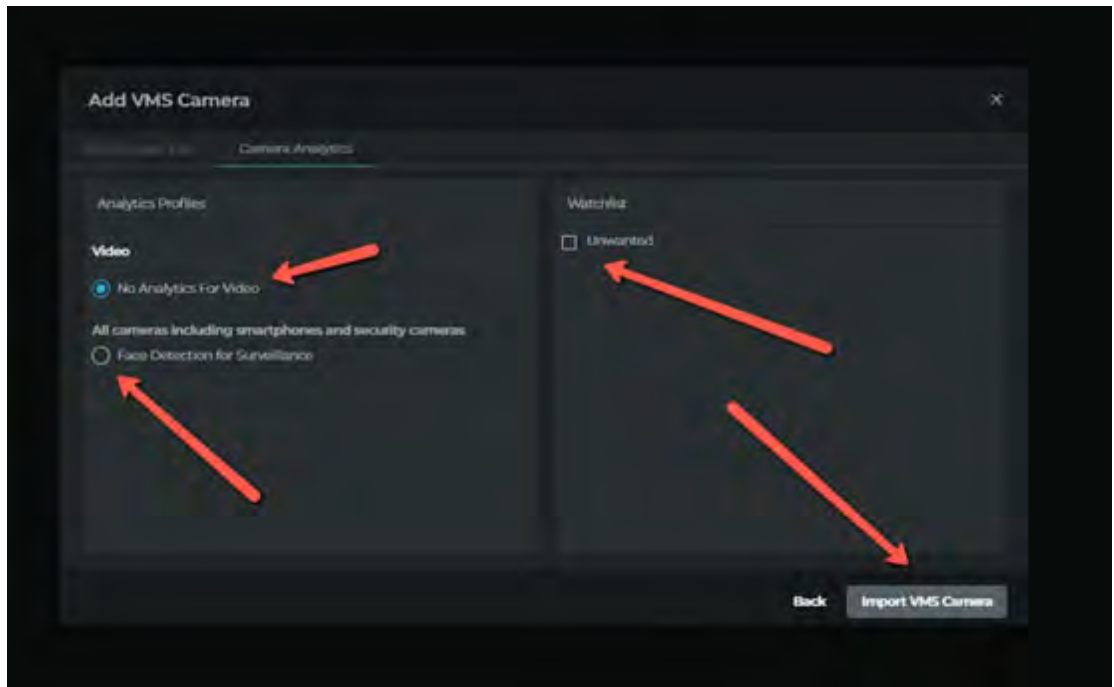
1. Log in to AV using the Google Chrome web browser with Username: "test" and Password: "test123!".

The following AV items should be configured before adding a VMS Camera to the system: There are connections needed to these items, hence do not skip these:

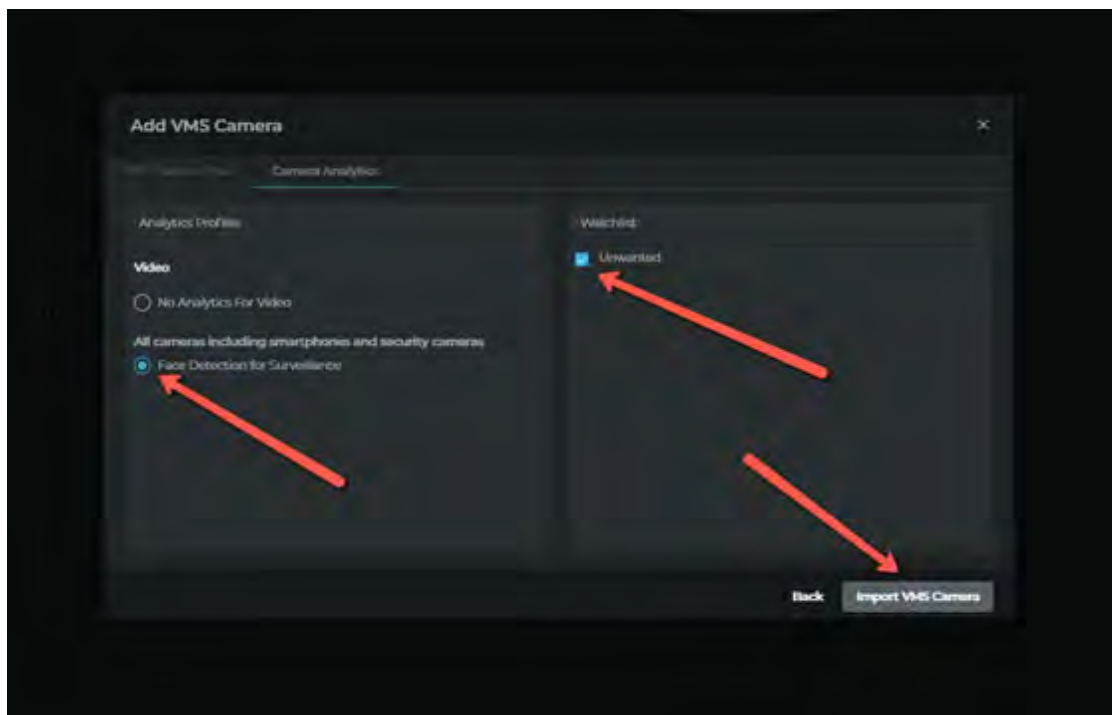
- An AV case must be created.
- An AV watch list must be created.
- There should be a few enrollment candidates in the watch list.

Step 6:

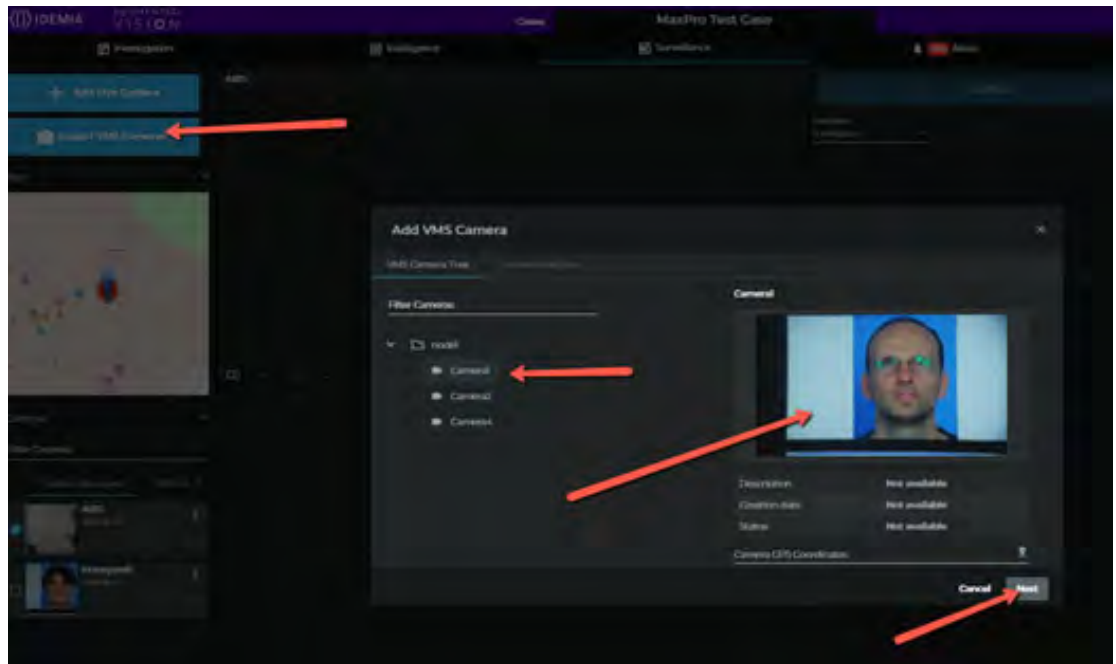
1. Click the Surveillance tab and then click the Import VMS Camera tab on the left pane. A list of the available cameras running on the Honeywell system is displayed.
2. Select the required camera and then click the Next button. The current selection in the image shows "No Analytics For Video".



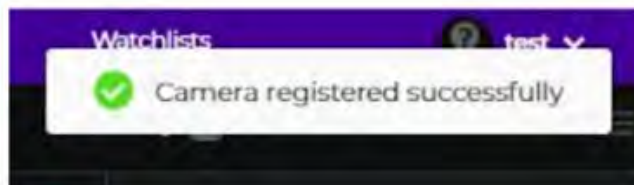
3. Select Face Detection for Surveillance and then select the watch list to be used for this camera.



4. Click the Import VMS Camera .

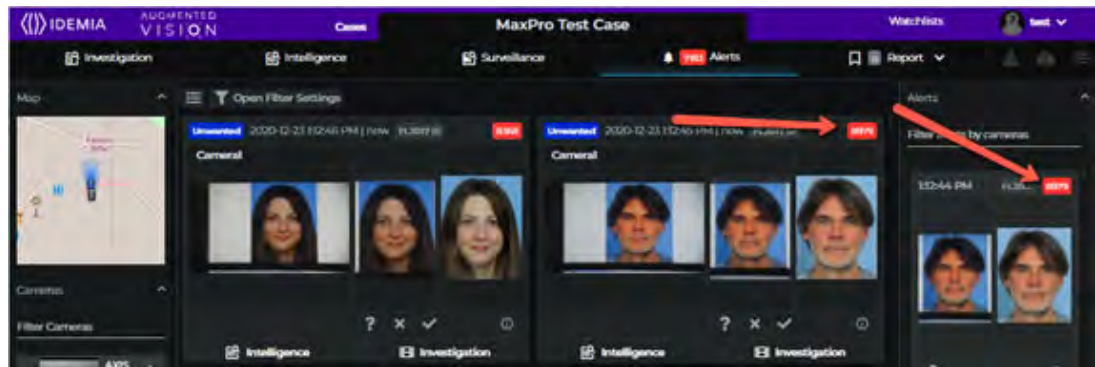


- Ensure that the following three messages appear on the right hand top corner of the screen, indicating that the adding camera process was successful:
 - Camera Registered Successfully
 - Successfully Watch list
 - Successfully requesting start/stop camera recording or analytic profiles

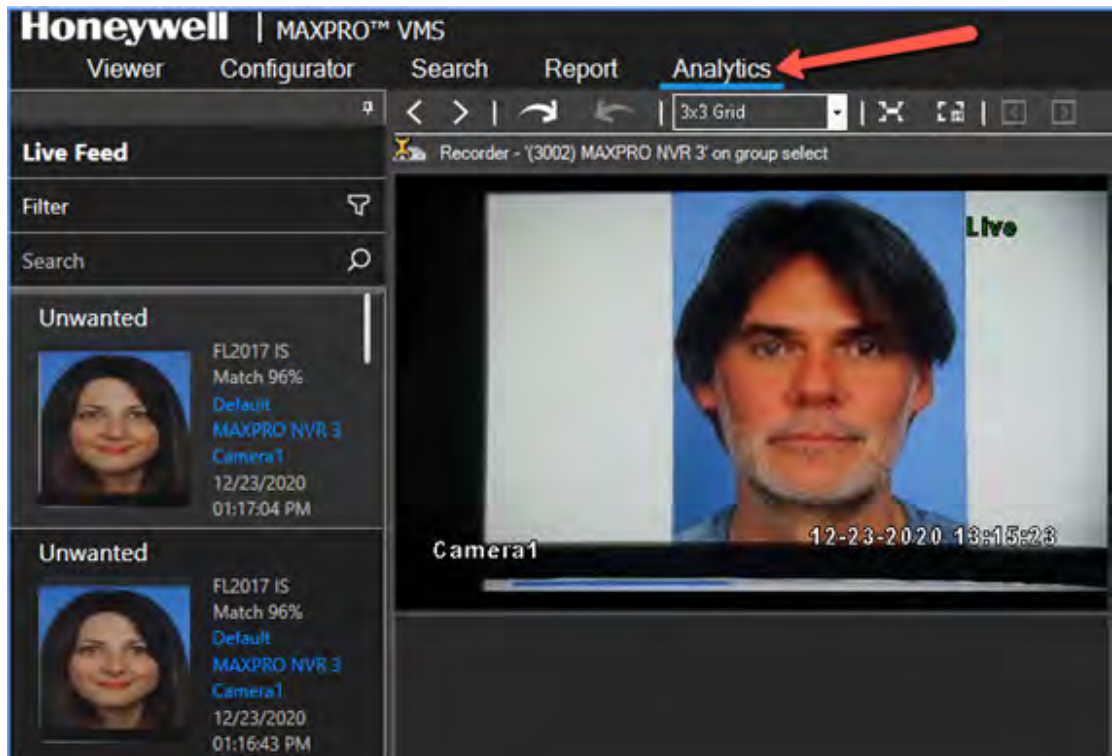


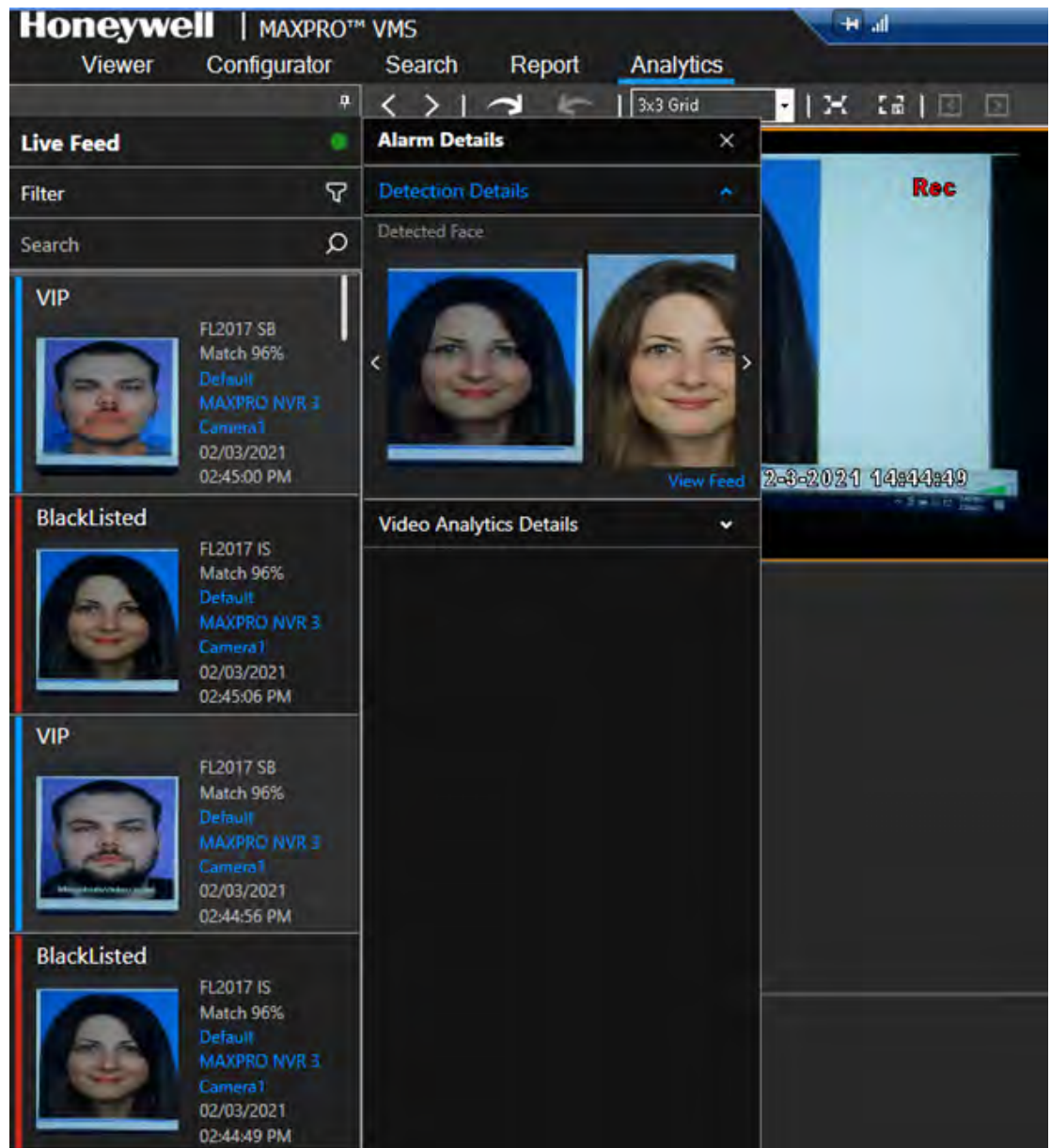
Step 7:

- Individuals identified will create an alert in AV and observed under the Alerts selection of AV as highlighted in Red.
- Adjudications displayed under the alerts selection in Orange are not alerts. Alerts sent to the VMS and can be seen under the Analytics tab of the VMS screen as shown below.



Alerts in MAXPRO VMS > Analytics tab.





VERIFYING THE CONFIGURATION OF MAXPRO VMS

Overview

Verifying the configuration of the MAXPRO VMS is the final phase in the commissioning process. In this phase, you need to verify the working of the MAXPRO VMS.

Before you begin

Ensure that the configuration of the MAXPRO VMS is complete.

Activities to perform

In this phase, using the MAXPRO VMS user interface, perform the tasks listed in the following table to verify the configuration in VMS Server.

Task	See...
Connection with the MAXPRO VMS server (logging on)	page 416
Device listing in the Devices window	page 417
Live video display from cameras	page 418
Playback of recorded video	page 418
Inserting comments and marking the point of interest using the bookmark feature in Timeline window	page 420
Playback of loop (mark in and mark out feature) in Timeline window	page 420
Panning, tilting, and zooming functions (analog PTZ and Digital PTZ)	page 421
Acknowledgment of alarms and clearing of alarms	page 421
Image creation	page 423
Clip creation	page 424
Sending and receiving operator messages	page 425

Task	See...
Video from the surrounding cameras (video pursuit or surrounding cameras feature in MAXPRO VMS)	page 425
Saving the salvo layout using the salvo view feature	page 426
Device listing in My Devices window	page 426
Searching recorded video	page 427
Generating and viewing the event and operator log report	page 427

Checking the Connection with VMS server

The MAXPRO VMS can consist of one or more servers. You can save the address of each server in profiles from the Log On page that appears when you start MAXPRO VMS. The Log On page is illustrated in the following figure.

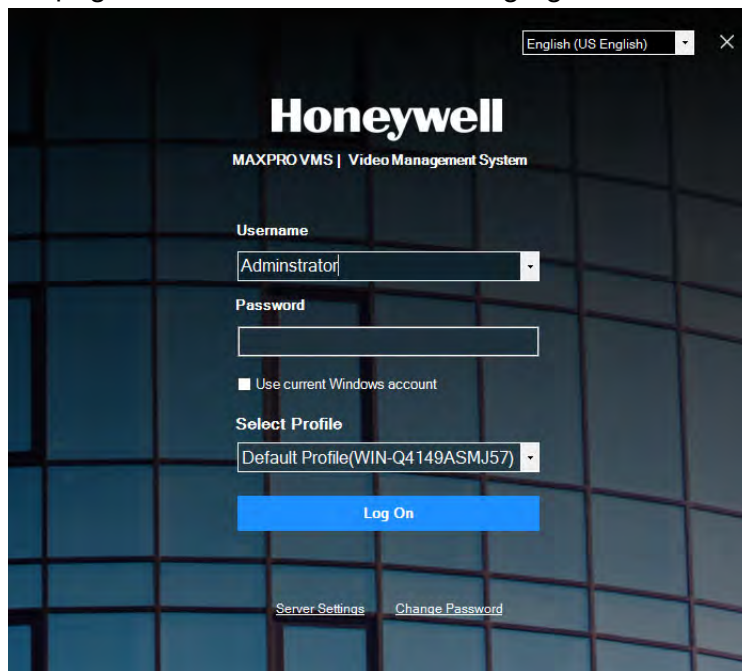


Figure 5-1 MAXPRO VMS Log on

To connect to a MAXPRO VMS R600 server from the client computer

1. Click the language selection option, and then select the required language from the drop-down list. The supported languages are Chinese, German, French, and Arabic. The default language is English.

Note: You can localize the language using the localization tool. For more details, refer to the [MAXPRO VMS Localization Guide](#) which is available on the DVD.

2. In the Username box, type the user name.
3. In the Password box, type the password.

4. In the Profile box, select the profile in which the server address is saved.
5. Click **Log On**. The MAXPRO VMS page is displayed.

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 VMS. You can also modify and delete profiles.

Note: Refer to the [MAXPRO® VMS Operators Guide](#) 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 profiles.

Checking the Device Listing

By default, the Viewer tab is selected when you log on to MAXPRO VMS. The Devices window lists the recorders, and switchers along with the cameras connected to them in a tree structure. Similarly sequences are listed in the Sequences window, salvo views are listed in the Views window, and monitors are listed in the Monitors window. A drop-down box on the top of the Devices window and Monitors window lists the partitions. The following figure illustrates the Viewer tab.

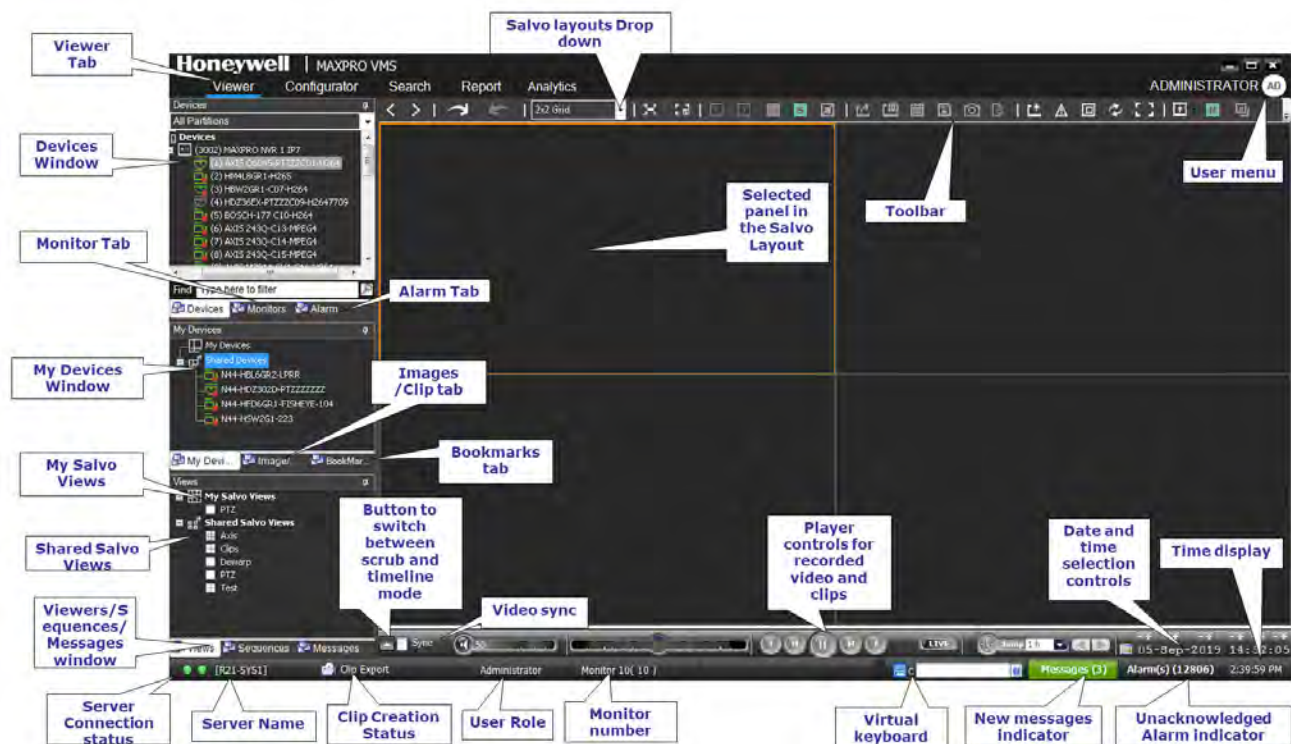


Figure 5-2 Viewer tab

Ensure that all the devices, sequences, and salvo views added to the MAXPRO VMS are listed in the respective windows.

To view the list of devices, monitors, sequences, and salvo views that are added:

- Click the required tab, in the Viewer. The devices, monitors, sequences, and salvo views are displayed in a tree view. For example, if you want to view the sequences, click the Sequences tab. The Sequences window appears with the list of sequences displayed in a tree structure. The sites that are associated to the monitors are also displayed in the Monitors window.

To view the list of devices and monitors for all the partitions

- In the drop down box, on the top of the Devices window, select All Partitions. The devices associated to the partition are displayed. Similarly, on the top of the Monitors window, select All Partitions. The monitors associated to the partition are displayed. The icons next to the devices in the Devices window indicate the status and type of each device.

Note: Refer to the [MAXPRO® VMS Operators Guide](#) for more information on the Viewer tab.

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 the camera in the Devices window or My Devices window. You can also drag the camera on a panel in the salvo layout. The panel starts displaying live video and the label Live appears over the video display.

The camera can also be selected using the virtual keyboard and joystick controller. You can select multiple cameras and view live video in different panels of the salvo layout.

Note: Refer to the [MAXPRO® VMS Operators Guide](#) 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. You can find out the status of the camera by the colored indicator on the camera icon in the site view. If the indicator on the camera icon is green means the camera is active. If the indicator on the camera is red means it is recording.

Note: Refer to the [MAXPRO® VMS Operators Guide](#) for more information on how to configure the recording settings for the cameras connected to the various recorders.

Recorded video can be played from the Timeline window. The following figure illustrates the Timeline window.

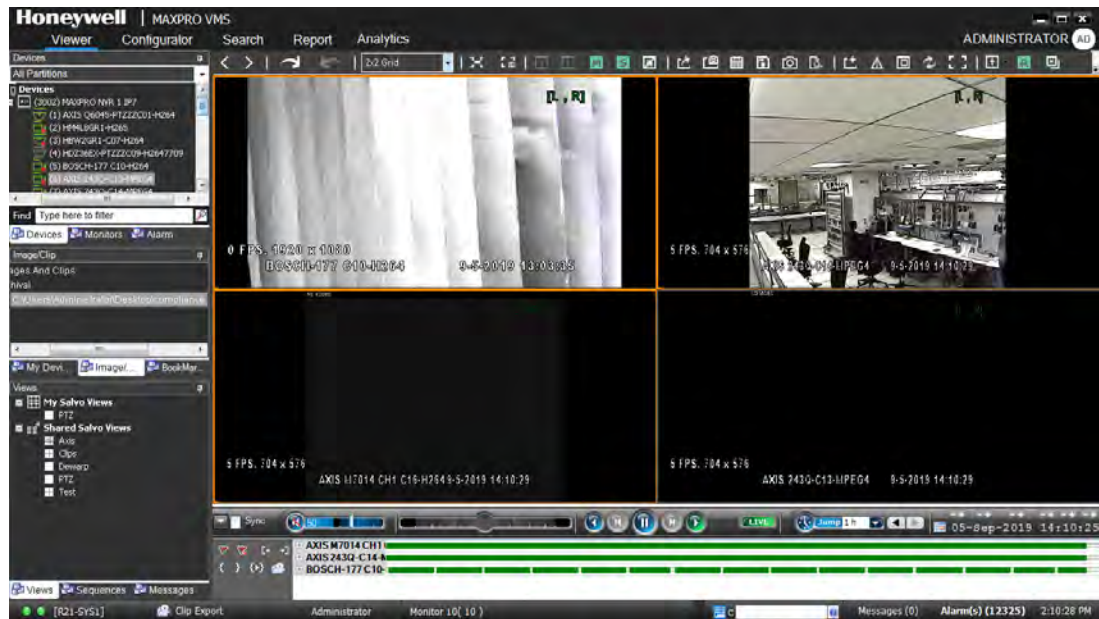


Figure 5-3 Timeline window

When you select a camera to view video, a timeline corresponding to the camera appears in the Timeline window. The name of the camera appears on the left of the timeline.

To play recorded video from a camera, you can click the timeline at the point from which you want to play video. A timescale is displayed in the lower part of the Timeline window. You can refer to the divisions in the timescale to locate the date and time. You can also select a date and time from which you want to play recorded video using the date and time options in the timeline window.

Color codes are used in the timeline to indicate the availability of video recording for the cameras connected to the recorder. The time duration for which recording is available is indicated in green color. The time duration for which recording is not available is indicated in white color.

For cameras connected to other recorders such as Rapid Eye, Fusion, Enterprise, Embedded Recorder and Intellex, the color codes are not displayed in the timeline. However, you can click a point in the timeline to play recorded video.

The label Rec is displayed in red color on the panel displaying recorded video from a camera.

Note: For more information on how to play recorded video from the Timeline window and how to use the player controls, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Bookmark Feature

The bookmark feature is used for marking points of interest in a video recording. Comments are added to the bookmarks and they appear as ToolTips in the timeline at marked points.

They are helpful while reviewing recorded video. The bookmarks can be cut or copied and pasted at different points in the timeline.

Operators can selectively view video by browsing from one bookmark to another in a timeline. The following figure illustrates bookmarks added to the timeline

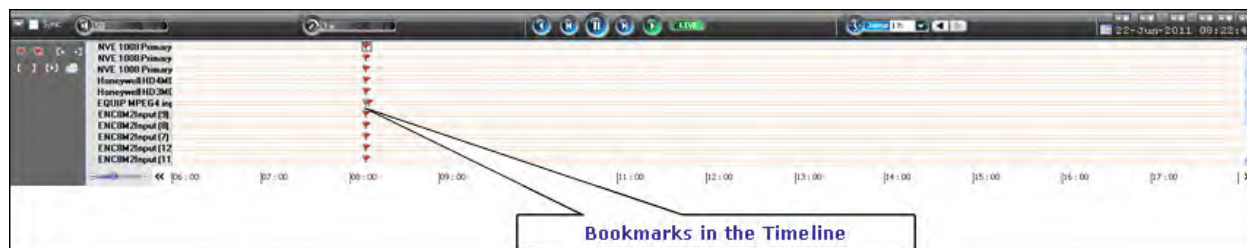


Figure 5-4 Bookmarks

Note: For more information on how to add, edit, cut, copy, paste, and delete bookmarks and on how to browse between bookmarks, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Playback Loop in Timeline

Loops are used for repeatedly playing a portion of video. Mark in and mark out points are used to create a loop in the Timeline window. You can add a mark in point to mark the start date and time of the loop in the timeline. To mark the end date and time of the loop, add a mark out point in the timeline. The following figure illustrates a loop in the timeline.



Figure 5-5 Loops

Note: For more information on how to create loops by adding mark in and mark out points and how to play a loop, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the PTZ Functions

In MAXPRO VMS, you can perform two types of PTZ namely, analog PTZ and Digital PTZ. Using the digital PTZ feature in MAXPRO VMS, you can perform tilting and zooming on live and recorded video and clips. You can also perform panning operations on live 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.

You need to perform both analog and digital PTZ on cameras to verify the functioning.

Note: For more information on how to perform analog and digital PTZ, refer to the [MAXPRO® VMS Operators Guide](#).

Checking for Acknowledgment and Clearing Alarms

Alarms notify the occurrence of events and event attributes 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 event attributes that are associated to events are listed in the details of the alarm in Alarm window. The events that trigger an alarm can be selected while configuring the recorders, cameras, and switchers. 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. The following figure illustrates the Alarm window.

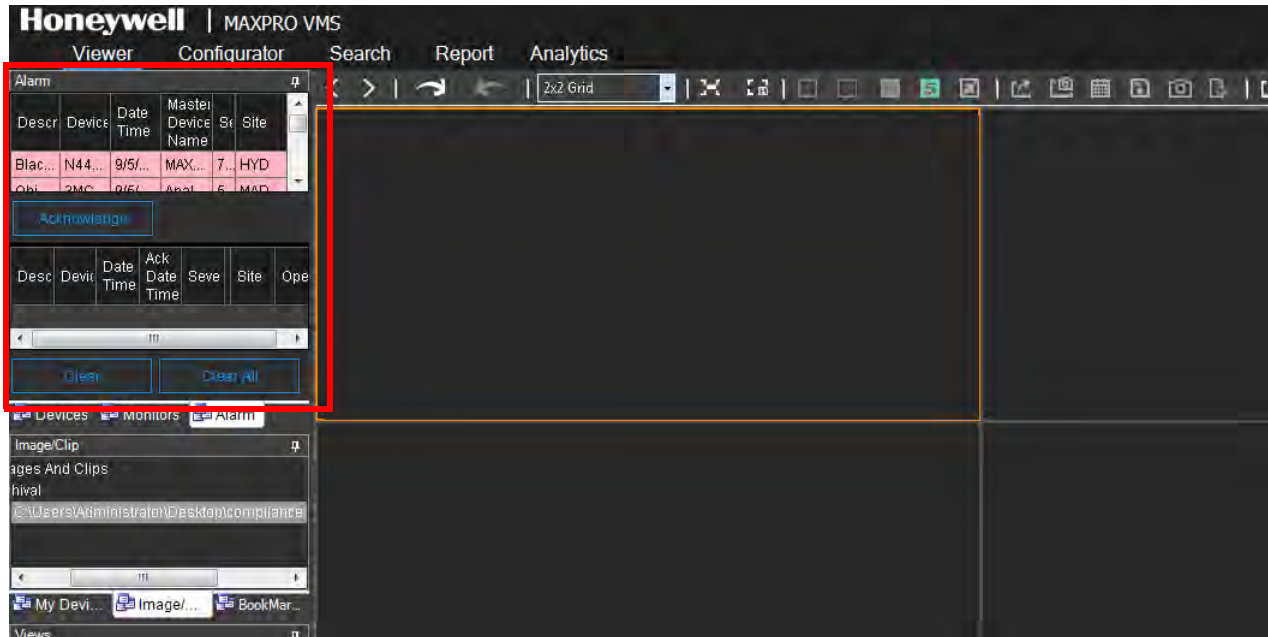


Figure 5-6 Alarm window

The number of unacknowledged alarms is displayed in a blinking mode in the status bar in red color. For example, Alarms (10) indicate that there are ten unacknowledged alarms. You can select various options using the context menu or shortcut menu by right clicking on the Alarms window. The options include:

- Acknowledge (ACK)
- Clear on ACK
- Ack all
- Show Video
- Show Preview Pane
- Show Details
- Freeze
- Receive Alarms Only
- Receive Events Only
- Receive both Alarms and Events

Acknowledge

An acknowledged alarm indicates that the operator has taken the action. After acknowledging the alarm, it is moved to the acknowledged alarms list in the Alarm window. You can also use the Acknowledge button below Alarms window. To clear acknowledged alarms, use the Clear button below Acknowledged list window.

Clear on ACK

This option clears the alarms which are acknowledged.

Ack all

This option acknowledges all the alarms at once.

Show Video

Select this option if you want to view video from which the alarm was generated.

Show Preview Pane

This option gives you four windows which display alarms which are on, pre-alarm, post alarm, and live alarm videos.

Show Details

This option displays the Alarm Details window. The Alarm Details window displays the details of description of the alarm, Device name, Date time, Alarm State, Global Event ID and the Event attributes.

Freeze

Select this option if you no longer wish to receive alarms.

Receive Alarms Only

Select this option if you want to receive only alarms.

Receive Events Only

Select this option if you want to receive only Events.

Receive both Alarms and Events

Select this option receive both alarms and events.

Note: For more information on how to acknowledge and clear alarms, refer to the [MAXPRO® VMS Operators Guide](#).

Checking for the Creation of Images

A frame of video displayed in the panel can be saved as an image. The image can be saved in Bitmapmed Graphics (BMP), Joint Photographic Experts Group (JPG) format, Portable Graphics format (PNG), and Graphics Interchange Format (GIF).

Only the images saved in the ImagesAndClips folder at the location in the hard drive in which MAXPRO VMS files are installed can be viewed in the Image/ Clip window. You can double-click the image view option in the Image/Clip window to view images on the salvo layout. You can also select the image size large, medium, and small as per the requirement.

For example, X:\ProgramFiles\Honeywell\TrinityFramework\ImagesAndClips.
Here, X: is the disk drive.

The following figure illustrates the Image/Clip window.

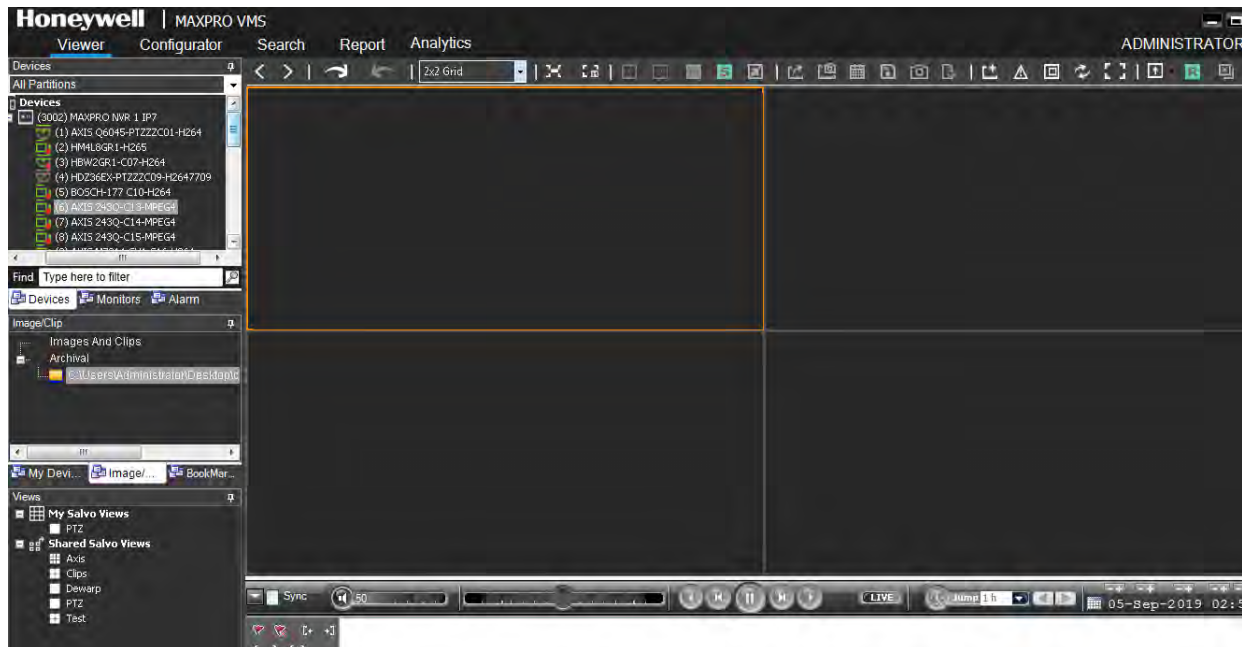


Figure 5-7 Image/Clip window

The images can also be saved in other folders on the computer.

Note: For more information on how to save and view images, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Creation of Clips

Clips can be created from recorded video and saved in MP4, MPG, AVI, and WMV format depending on the format supported by the recorders. Only the clips saved in the ImagesAndClips folder at the location in the hard drive in which MAXPRO VMS files are installed can be viewed in the Image/ Clip window.

For example, X:\ProgramFiles\Honeywell\TrinityFramework\ImagesAndClips. Here, X: is the hard drive.

The clips can also be saved in other folders on the computer.

The 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 World Wide Web Consortium (W3C) 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.

Note: For more information on how to save and view images, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Sending and Receiving of Operator Messages

Operator messaging enables operators to send video displayed in one or more panels or the whole salvo layout to other operators and digital monitors. Comments can be included in the message sent to operators. The comments are not included when the message is sent to digital monitors. The received messages can be viewed in the Messages window.

The number of new messages appears in the blinking mode in the status bar. For example, Messages(3) in green color indicates three new messages. The following figure illustrates the Messages window.

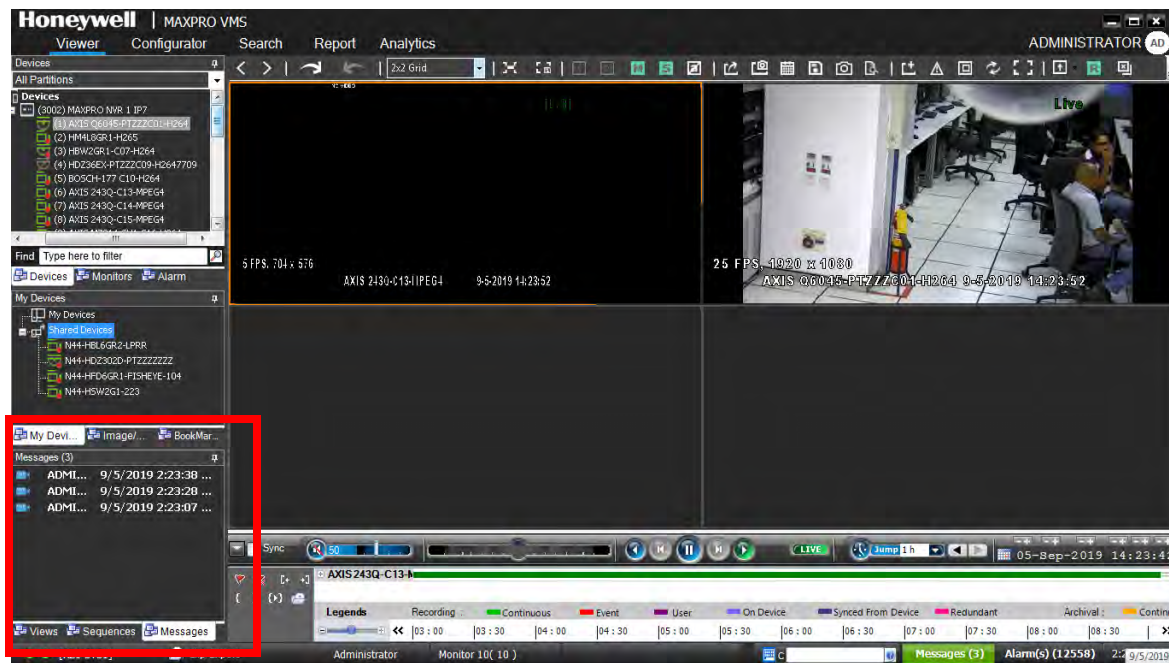


Figure 5-8 Messages window

Note: For more information on how to send and receive messages, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Surrounding Cameras Feature

A camera can be associated to a group of cameras using the surrounding cameras feature. This feature enables operators to view video from a group of related cameras at the same time. For example, video from cameras located in the same area.

Note: For more information on how to associate camera and how to view video from a group of related cameras, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Saving of Salvo Layout

A salvo layout that is customized based on the preferences of the operators is referred to as a salvo view. Cameras and sequences that are selected frequently and the preferred salvo layout can be saved as a salvo view. The saved salvo views appear in the Views window.

Note: For more information on how to create, select, and manage salvo views, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Device Listing in My Devices

In the My Devices window, operators can group the video sources, which are frequently selected such as cameras, monitors, and sequences. If you group the video sources, it is easy to select and you need not search in the Devices window, which generally consists of many video sources. You can also group the devices under shared devices. Devices grouped under shared devices are displayed on all client workstations irrespective of the logged in user.

The following figure illustrates My Devices window.

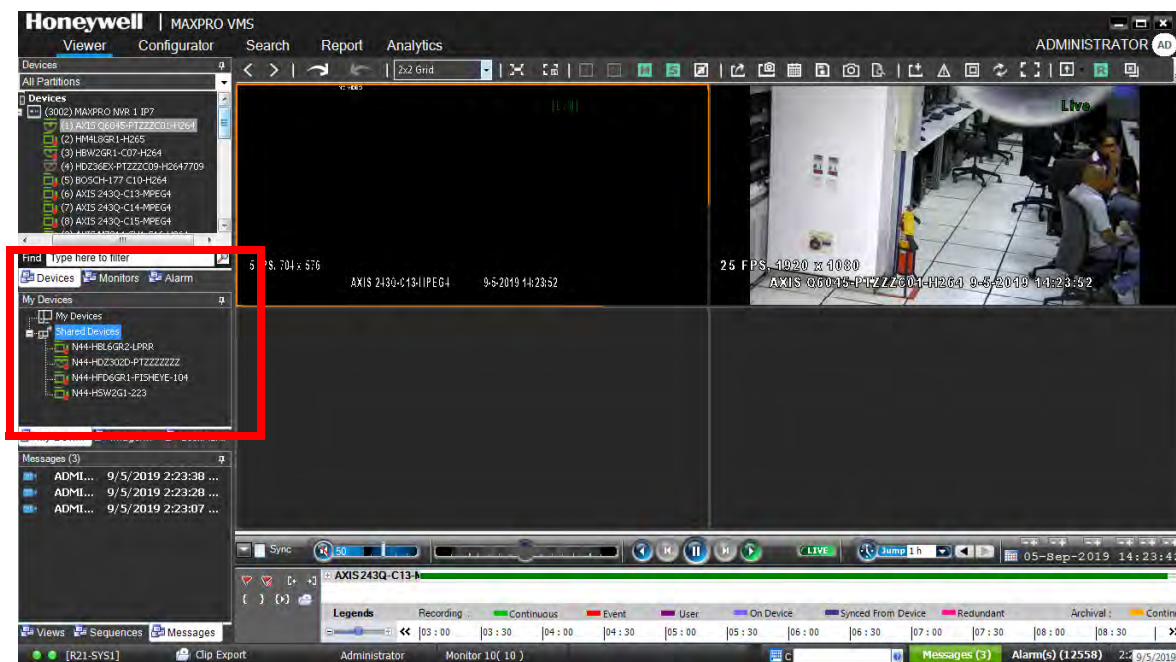


Figure 5-9 My Devices window

Note: For more information on how to add a video source to My Devices window and how to create folders to group them, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Search for Recorded Video

Operators can search for recorded video, events, bookmarks from cameras connected to the recorders. The Search tab looks similar to the following figure.

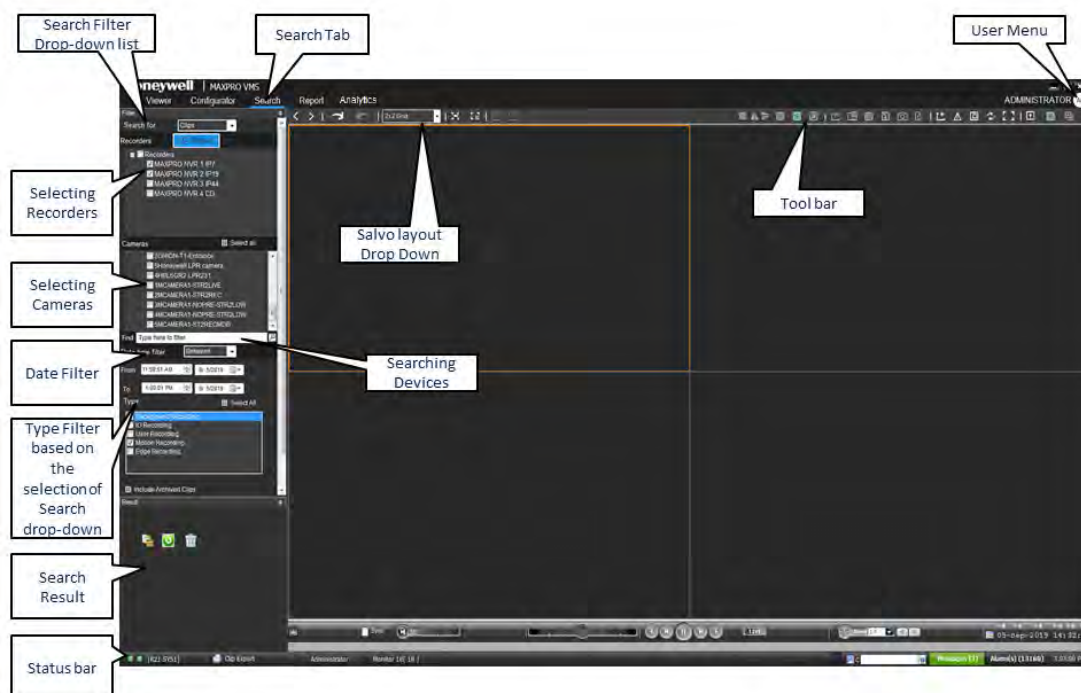


Figure 5-10 Search tab

Note: For more information on how to search for recorded video, clips and bookmarks and how to play the search results, refer to the [MAXPRO® VMS Operators Guide](#).

Checking the Generation of Reports

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, recorders, and switchers. 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 others.

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, sending messages and other actions performed by a user.

You can generate reports from the Report tab. The following figure illustrates the Report tab.

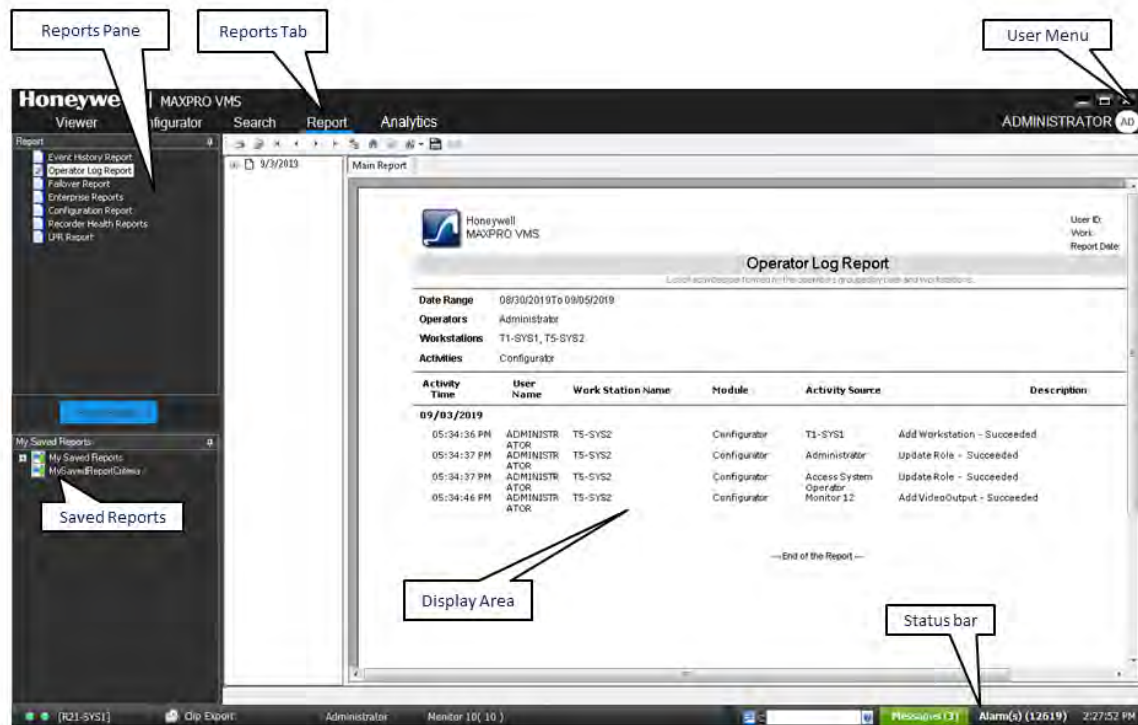


Figure 5-11 Report tab

Note: For more information on how to generate and view the reports, refer to the [MAXPRO® VMS Operators Guide](#).

UPGRADE MAXPRO VMS

Overview

This chapter describes various scenarios to upgrade the existing version of MAXPRO VMS to latest version. Follow the steps in respective sections to upgrade MAXPRO VMS software.

The following are the upgrade scenarios covered. Refer the specific sections to upgrade MAXPRO VMS

- Upgrading to MAXPRO VMS R670
- Upgrading to MAXPRO VMS R630
- Upgrading to MAXPRO VMS R600 B622
- MAXPRO® VMS R550 Build 558 to VMS R560 Build 573
- MAXPRO® VMS R500 SP1 Build 532 to VMS R550 Build 558
- MAXPRO VMS R500 Build 523 to R500 SP1
- MAXPRO VMS R500 Build 512 to R500 Build 523
- MAXPRO VMS R490 Build 495 to R500 Build 512
- MAXPRO VMS R470 Build 476 to R500 Build 512
- MAXPRO VMS R450 Build 455 to R500 Build 512
- MAXPRO VMS R410 Build 424 to R500 Build 512

Upgrade to MAXPRO VMS R670

- Upgrade to VMS R670 Build 687 is supported from the following version only.
 - MAXPRO® VMS R630 Build 643
 - MAXPRO® VMS R600 B622

Below tables explain the upgrade support to MAXPRO and Pro-Watch R670:

Upgrade Support	MNVR/MVMS 670	Retain License	Change to Demo License
MNVR/MVMS 600	✓	✓	✗
MNVR/MVMS 630	✓	✓	✗
PNVR/PVMS 650	✗	NA	NA
PNVR/PVMS 650 SP1	✗	NA	NA

Upgrade Support	PWNVR/PWVMS 670	Retain License	Change to Demo License
MNVR/MVMS 600	✓	✗	✓
MNVR/MVMS 630	✓	✗	✓
PWNVR/PWVMS 650	✓	✓	✗
PWNVR/PWVMS 650 SP1	✓	✓	✗

To upgrade to MAXPRO VMS R670

1. Browse to the setup folder and double-click MAXPRO VMS_R670 Setup. exe. The installer extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates.
2. Click Yes to disable and proceed. The Welcome page appears.
3. Click Continue. The installation process continues and once the installation is complete the completion page is displayed.
4. Click Finish to complete.

Upgrade to MAXPRO VMS R630

- Upgrade to VMS R630 Build 643 is supported from the following version only.
 - MAXPRO® VMS R600 B622

To upgrade to MAXPRO VMS R630

1. Browse to the setup folder and double-click MAXPRO VMS_R630 Setup. exe. The installer extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates.
2. Click Yes to disable and proceed. The Welcome page appears.
3. Click Continue. The installation process continues and once the installation is complete the completion page is displayed.
4. Click Finish to complete.

Upgrade to MAXPRO VMS R600

Upgrade to VMS R600 B622 is supported from the following versions only.

- MAXPRO® VMS R600- Build 615
- MAXPRO® VMS R600- Build 612
- MAXPRO® VMS R560- Build 573
- MAXPRO® VMS R550- Build 559
- MAXPRO® VMS R500 SP1 - Build 532
- MAXPRO® VMSR500 T-Patch - Build 523
- MAXPRO® VMS R500 Build 512

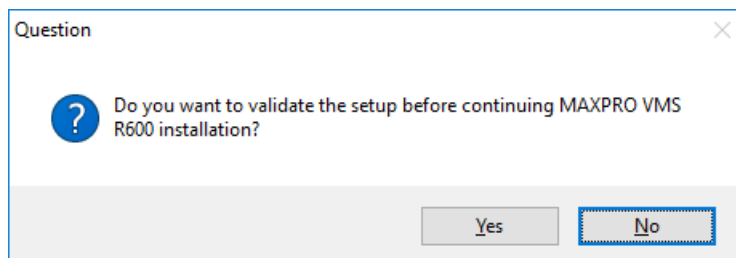
Pre-requisite

Before upgrading to MAXPRO VMS R600, user must install the below SQL service pack for successful upgrade. Refer to the [800-26010-A - Securing MAXPRO VMS-NVR Technical Notes](#) for more information on how to download and install the below service pack.

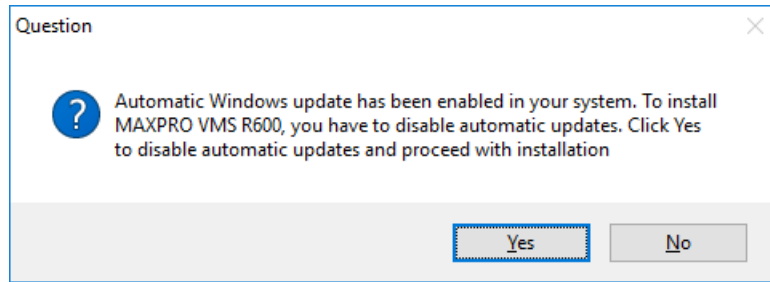
- SQL2014SP3

To upgrade to MAXPRO VMS R600 Build 622

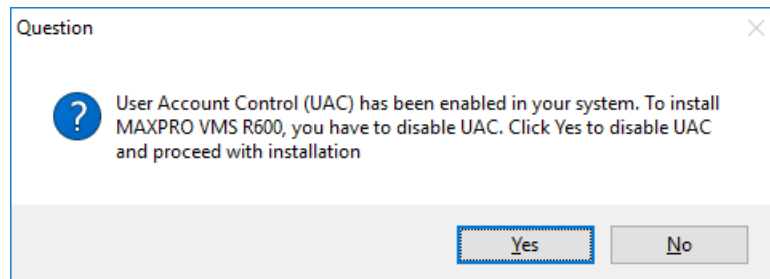
1. Insert the MAXPRO VMS R600 DVD in the DVD drive. The setup runs automatically. If the setup does not run automatically, browse to the setup folder on the DVD and double-click Setup. exe. Validation message appears as shown below.



2. Click Yes to validate or click No to continue without validation. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



3. Click Yes to disable and proceed. A UAC message is displayed as shown below.



4. Click Yes to disable the UAC. The Welcome page appears.

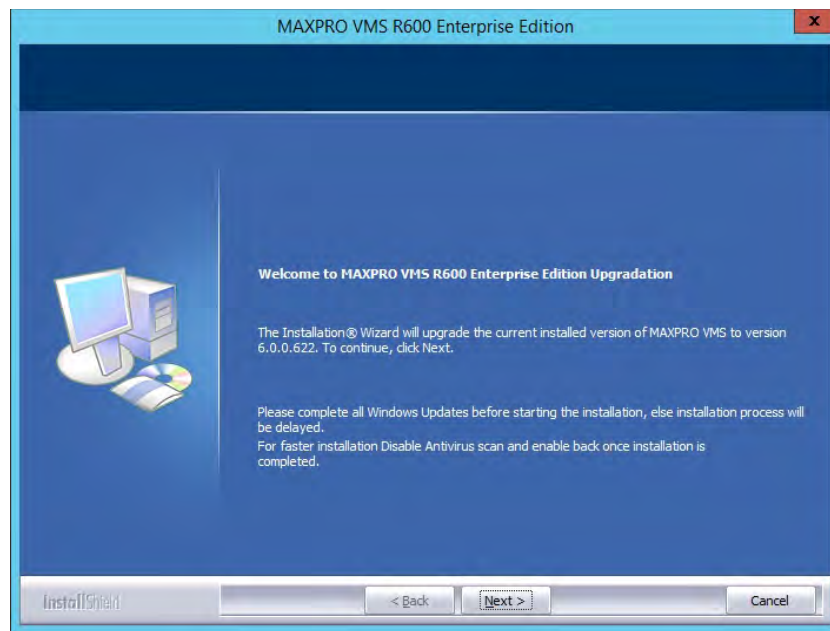


Figure 6-1 Welcome

5. Click Next. The Features to be upgraded page appears.

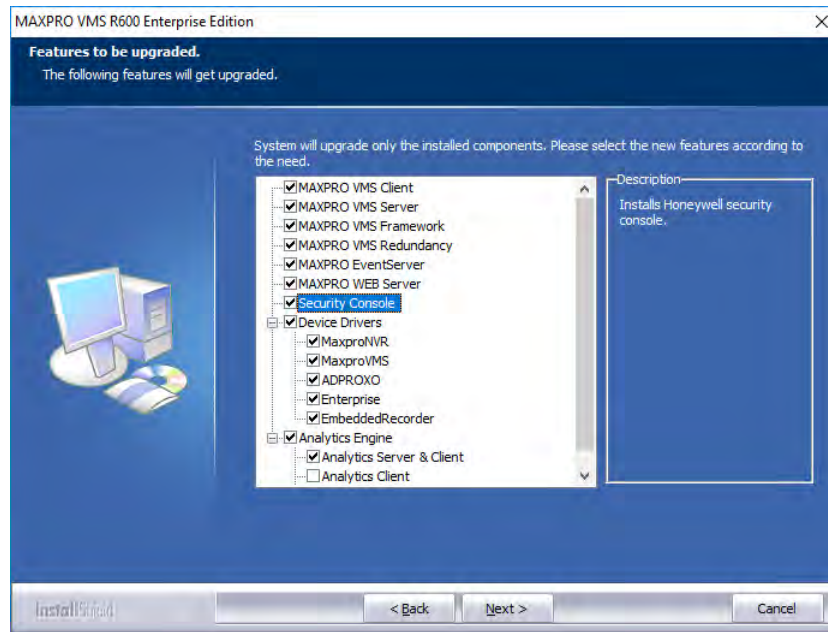
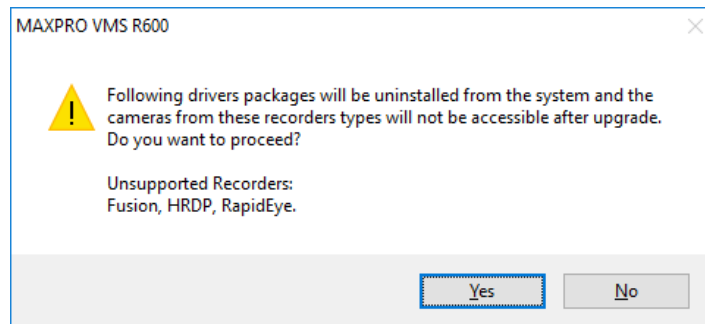


Figure 6-2 Features to be upgraded

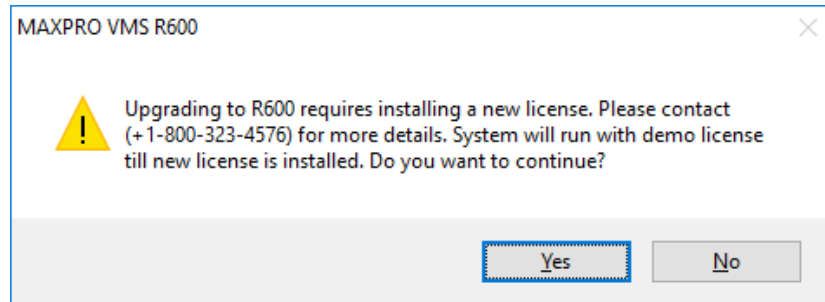
6. Select the new features you want to install/upgrade. Click the respective Server or Client check boxes. The check boxes for the features to be upgraded are selected by default.

Note: Clear the check boxes for the features that you do not want to install/upgrade. For example If you want upgrade only client then clear the Server check boxes and vice versa.

7. Click Next. A confirmation message box about the unsupported recorders is displayed as show below.



8. Read and click Yes to proceed. A confirmation message box about new license installation is displayed as shown below.



9. Read the message and click Yes to continue. The Validation of User Credentials page appears

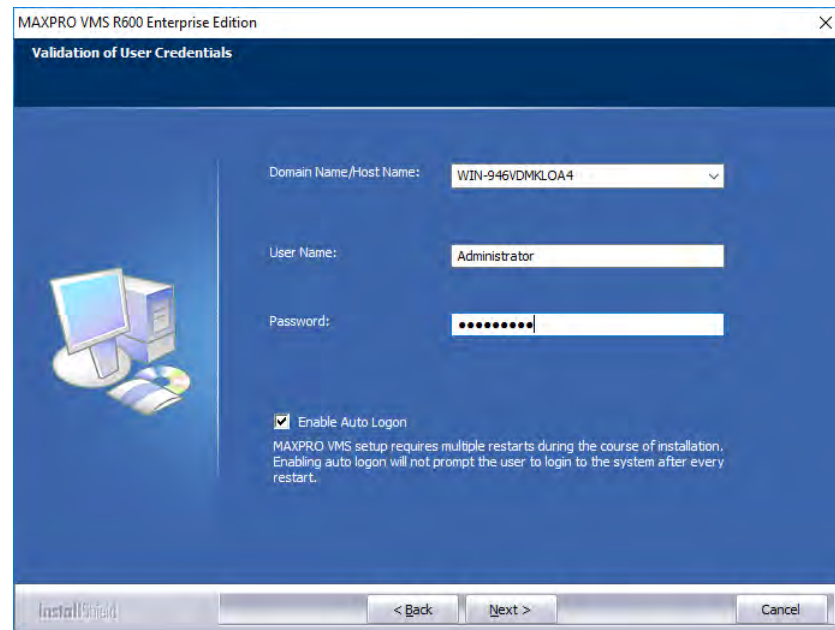


Figure 6-3 Validation of User Credentials

10. In the Domain Name/Host Name list, type the domain name or host name if you know it or select one from the list.
11. In the User Name box, type your Windows user name.
12. In the Password box, type your Windows password.
13. Select the Enable Auto Logon check box if you want the computer to reboot on its own whenever required, during the installation process.

Note: You are prompted to reboot multiple times while upgrading to MAXPRO VMS R600, auto log on avoids manual intervention during multiple reboots. A confirmation message is displayed as shown below. Click Yes to continue.



14. Click Next. The Choose Cache file location page appears.

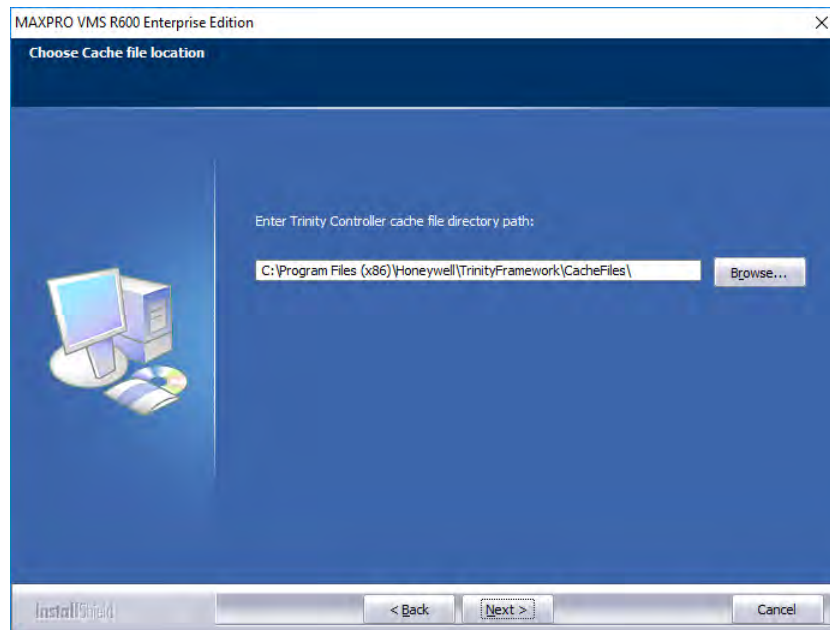


Figure 6-4 Choose Cache File Location

15. Click Next. The Language selection for analytics application page appears. For client upgrade language selection wizard is not displayed.

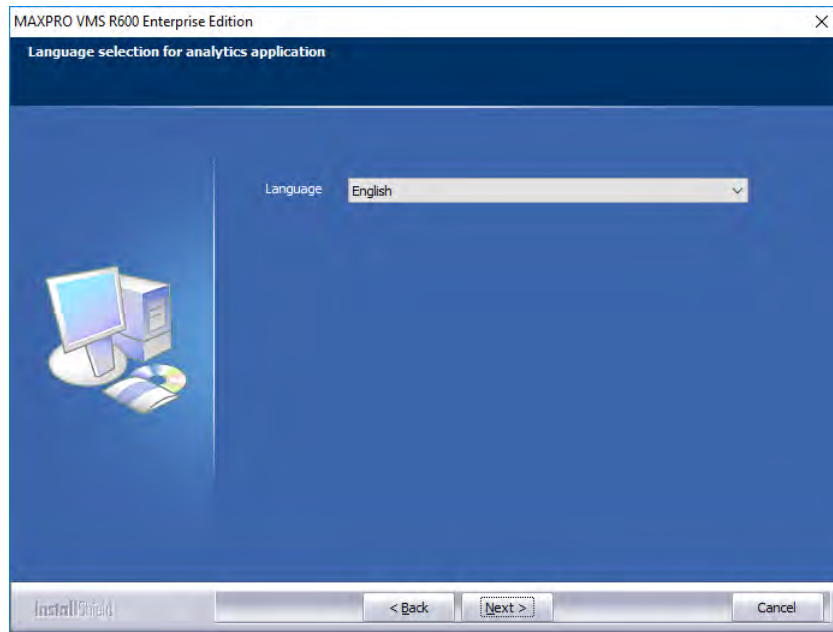
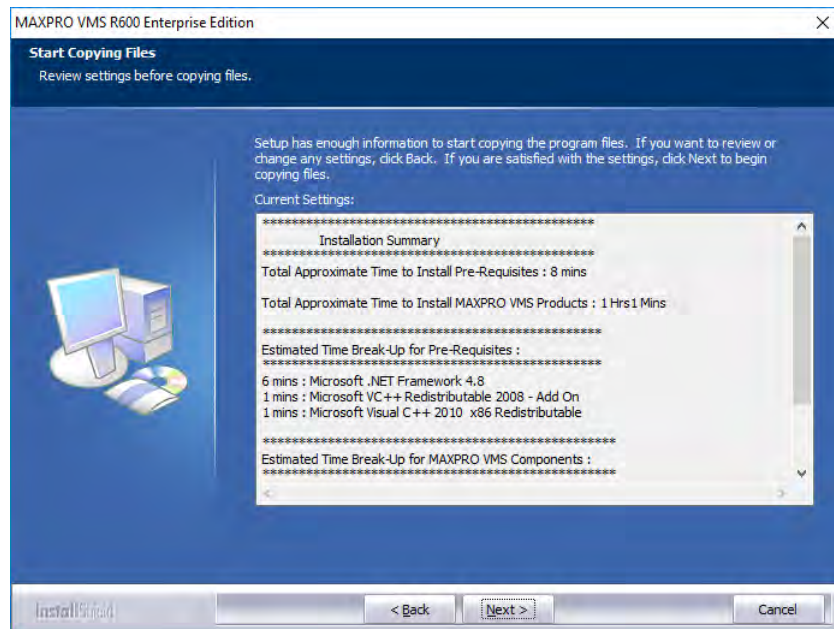
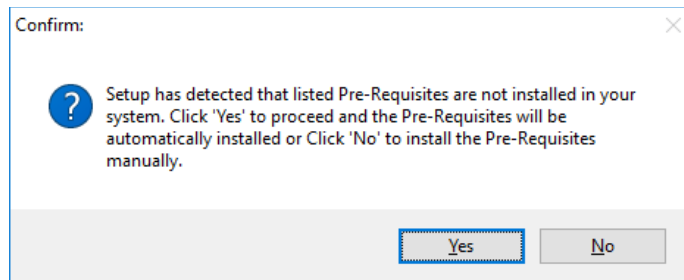


Figure 6-5 Language Selection

16. Select the Language from the drop-down list. Click Next, the Start Copying Files page appears.



Note: A confirmation message is displayed as shown below. Click Yes to proceed and to install the list of prerequisites.



17. Click Next. The status of various components is displayed. After the components are installed/upgraded successfully, the Upgrade Complete page appears.

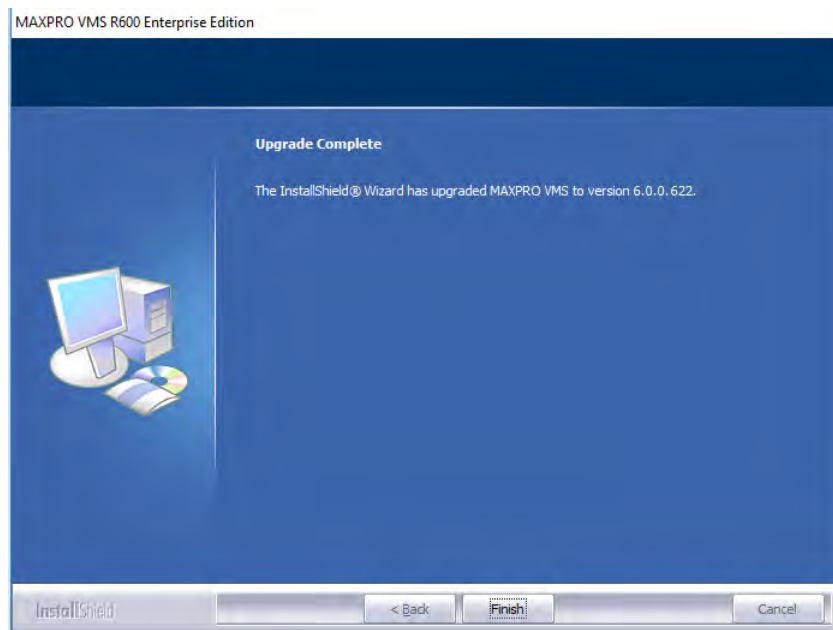


Figure 6-6 Upgrade Complete

18. Click Finish to complete the upgrade.

Upgrade to MAXPRO VMS R560

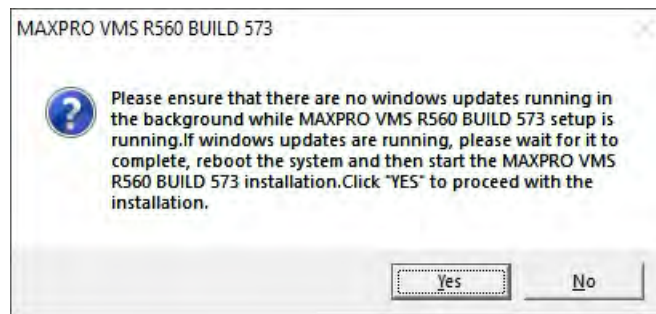
Note: This build (MAXPRO VMS R560) is recommended to install on a 64 bit OS Client machine.

- Upgrade to VMS R560 B 573 is supported from the following versions only.
 - MAXPRO® VMS R500 Build 512
 - MAXPRO® VMS R500_T Patch Build 523

- MAXPRO® VMS R500 SP1 Build 532
- MAXPRO® VMS R550 Build 558

To upgrade to MAXPRO VMS R560

1. Browse to the setup folder and double-click MAXPRO VMS_R560 Setup. exe. The installer extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



2. Click Yes to disable and proceed. The Welcome page appears.



3. Click Continue. The installation process continues and once the installation is complete the completion page is displayed as shown below.



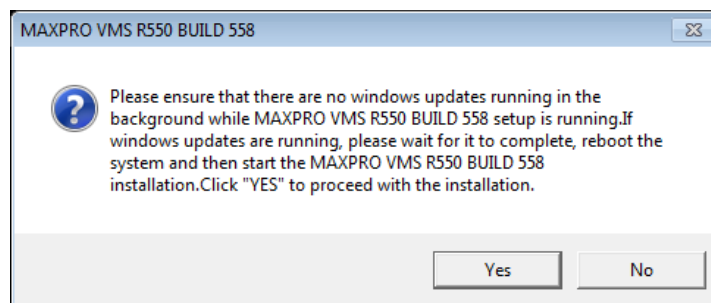
4. Click Finish to complete.

Upgrade to MAXPRO VMS R550

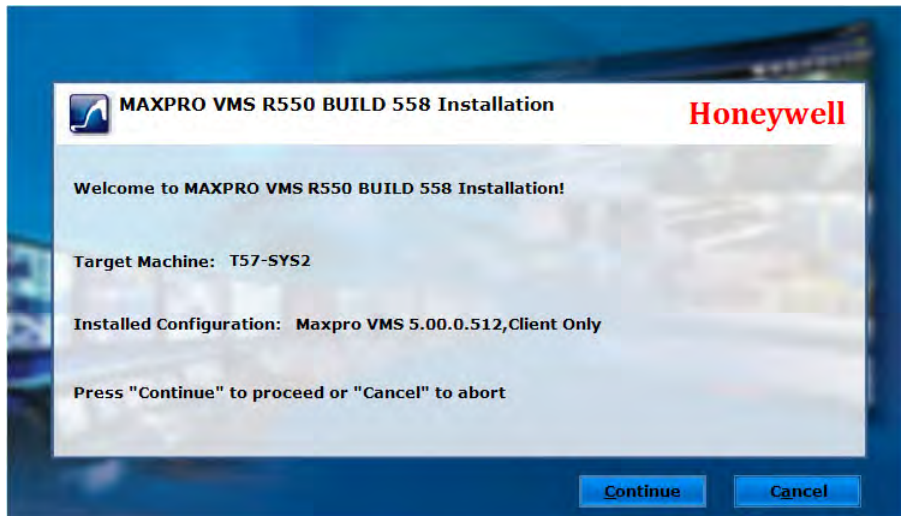
- Upgrade to VMS R550 is supported from the following versions only.
 - MAXPRO® VMS R500 Build 512
 - MAXPRO® VMS R500_T Patch Build 523
 - MAXPRO® VMS R500 SP1 Build 532

To upgrade to MAXPRO VMS R550

1. Browse to the setup folder and double-click MAXPRO VMS_R550 Setup. exe. The installer extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



2. Click Yes to disable and proceed. The Welcome page appears.



3. Click Continue. The installation process continues and once the installation is complete the completion page is displayed as shown below.



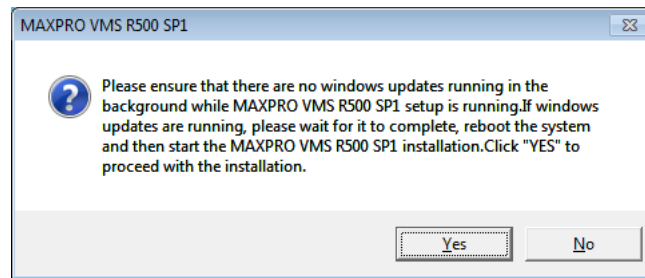
4. Click Finish to complete.

Upgrade To MAXPRO VMS R500 SP1

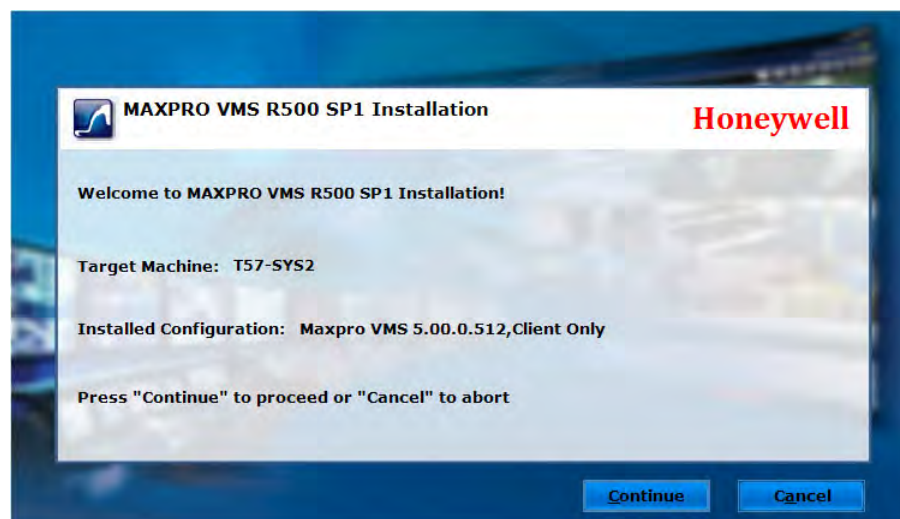
- Upgrade to R500 Service Pack 1 is supported from the following versions only.
 - MAXPRO® VMS R500 Build 512
 - MAXPRO® VMS R500 Build 523

To upgrade to MAXPRO VMS R500 SP1

1. Browse to the setup folder and double-click MAXPRO VMS_R500_SP1 Setup.exe. The installer extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



2. Click Yes to disable and proceed. The Welcome page appears.



3. Click Continue. The installation process continues and once the installation is complete the completion page is displayed as shown below.



4. Click Finish to complete.

Uninstalling SP1

In Add/Remove program windows there will be two entries as:

- MAXPRO_VMS_ 500_T patch Build 523
- MAXPRO_VMS_ 500 SP1 Build 532

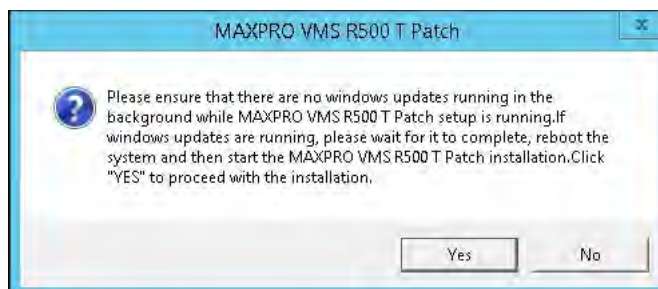
If user wants to go back to v500 Build 512 then from Add/Remove Program window perform an installation in the order as mentioned:

1. Uninstall SP1
2. Uninstall 500_T patch Build 523

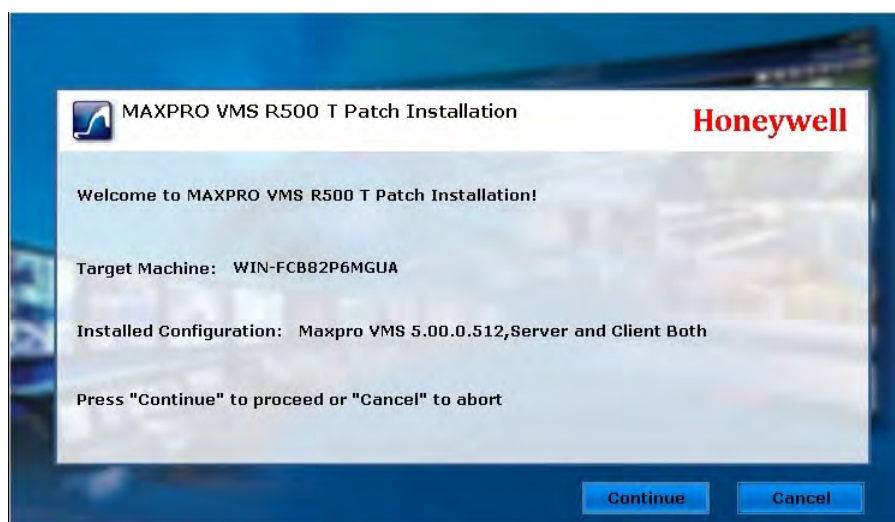
Upgrade MAXPRO VMS R500 Build 512 to R500 Build 523

To upgrade MAXPRO VMS R500 Build 512 to R500 Build 523

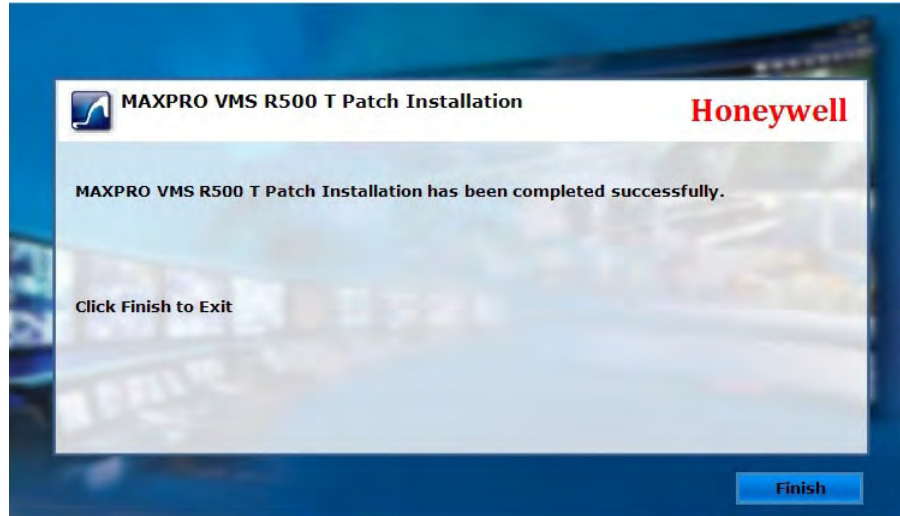
1. Browse to the setup folder and double-click MAXPRO VMS_R500_Build523 Patch Setup. exe. The WinRaR self extracting archive wizard appears and extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



2. Click Yes to disable and proceed. The Welcome page appears.



3. Click Continue. The installation process continues and once the installation is complete the completion page is displayed as shown below.

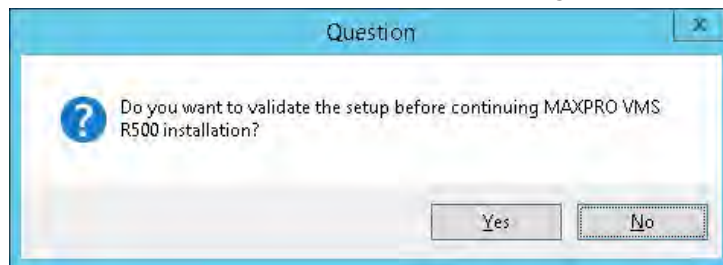


4. Click Finish to complete.

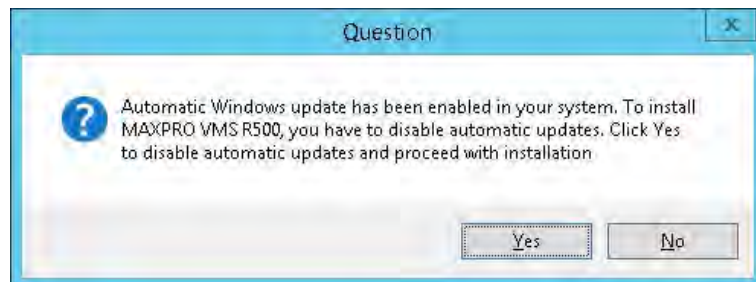
Upgrade to MAXPRO VMS R500

To upgrade to MAXPRO VMS R500 Build 512

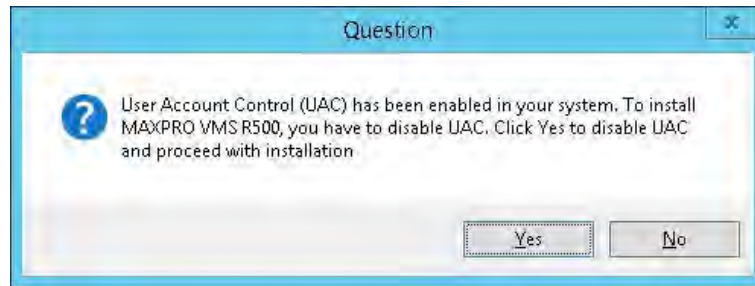
1. Insert the MAXPRO VMS R500 DVD in the DVD drive. The setup runs automatically. If the setup does not run automatically, browse to the setup folder on the DVD and double-click Setup. exe. Validation message appears as shown below.



2. Click Yes to validate or click No to continue without validation. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



3. Click Yes to disable and proceed. A UAC message is displayed as shown below.



4. Click Yes to disable the UAC. The Welcome page appears.

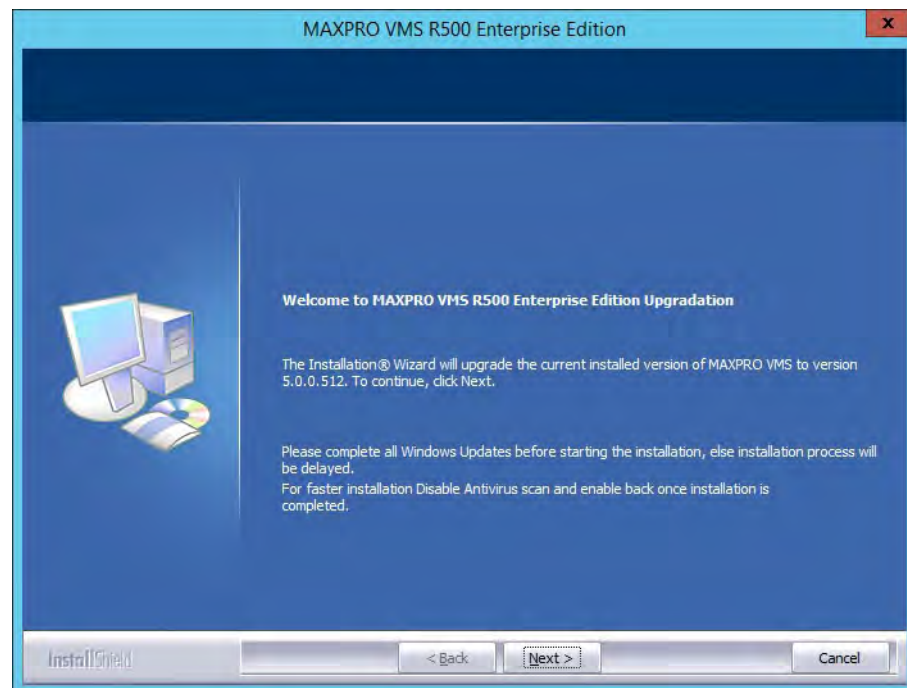


Figure 6-7 Welcome

5. Click Next. The Validation of User Credentials page appears

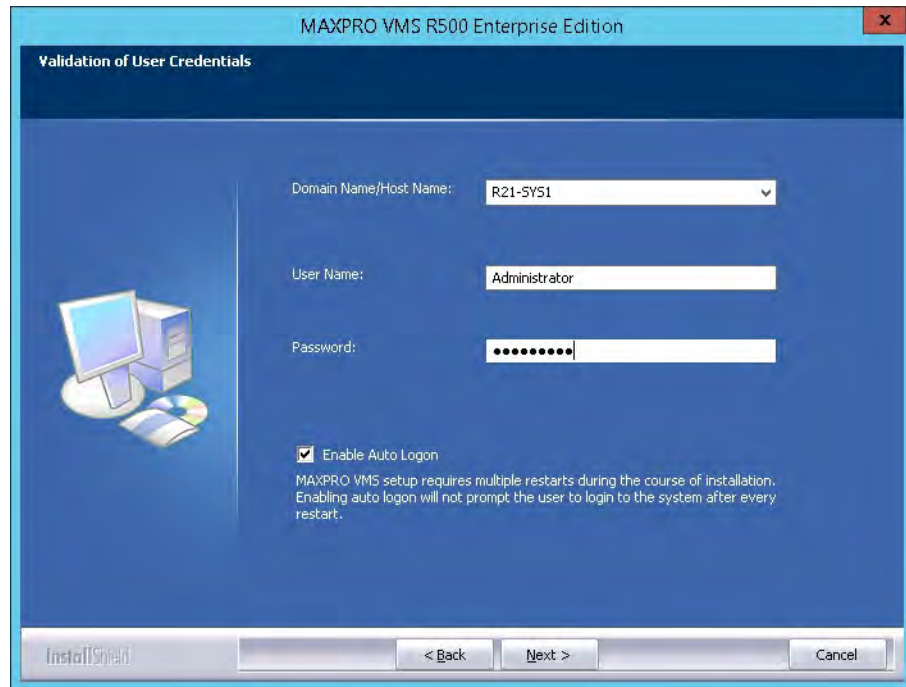
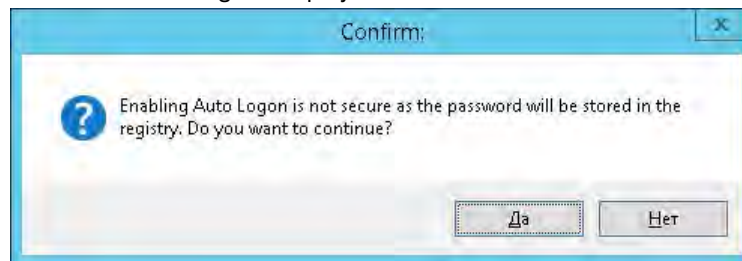


Figure 6-8 Validation of User Credentials

6. In the Domain Name/Host Name list, type the domain name or host name if you know it or select one from the list.
7. In the User Name box, type your Windows user name.
8. In the Password box, type your Windows password.
9. Select the Enable Auto Logon check box if you want the computer to reboot on its own whenever required, during the installation process.

Note You are prompted to reboot multiple times while upgrading to MAXPRO VMS R500, auto log on avoids manual intervention during multiple reboots. A confirmation message is displayed as shown below. Click Yes to continue.



10. Click Next. The Features to be upgraded page appears.

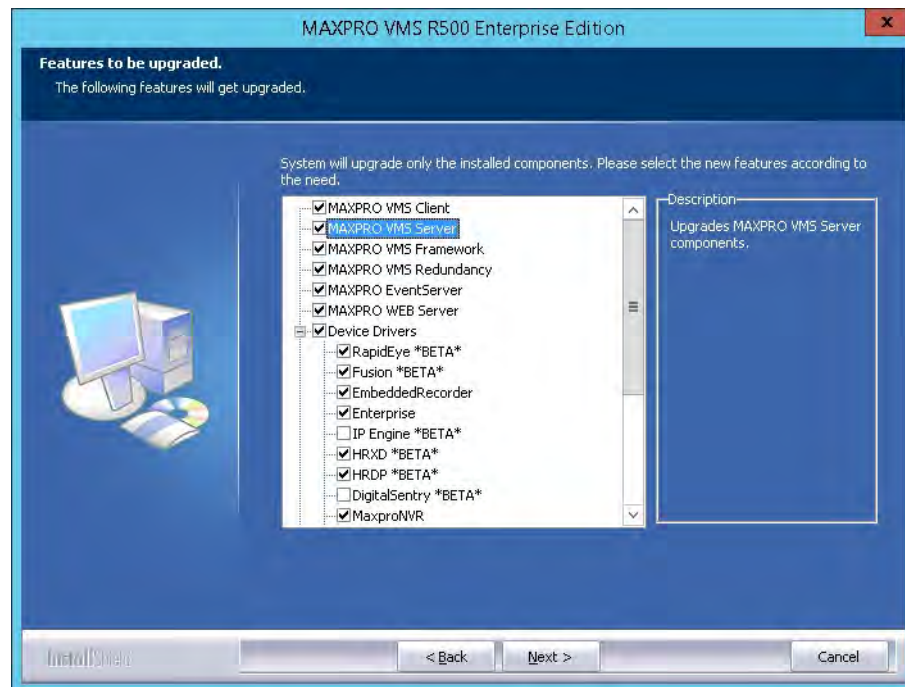


Figure 6-9 Features to be upgraded

11. The check boxes for the features to be upgraded are selected by default. Select the new features you want to install/upgrade. Click the respective Server or Client check boxes.

Note:

- Clear the check boxes for the features that you do not want to install/upgrade. For example If you want upgrade only client then clear the Server check boxes and vice versa.
 - A confirmation message about features of BETA version is displayed. Click **OK** to proceed.
-

12. Click Next. The Choose Cache file location page appears.

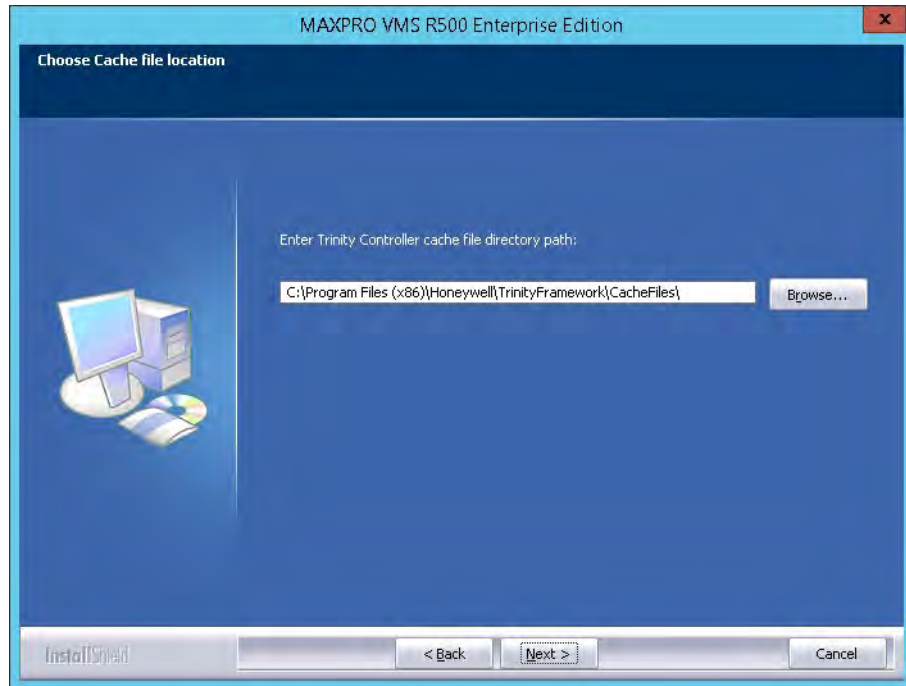


Figure 6-10 Choose Cache File Location

13. Click Next. The Language selection for analytics application page appears. For client upgrade language selection wizard is not displayed.

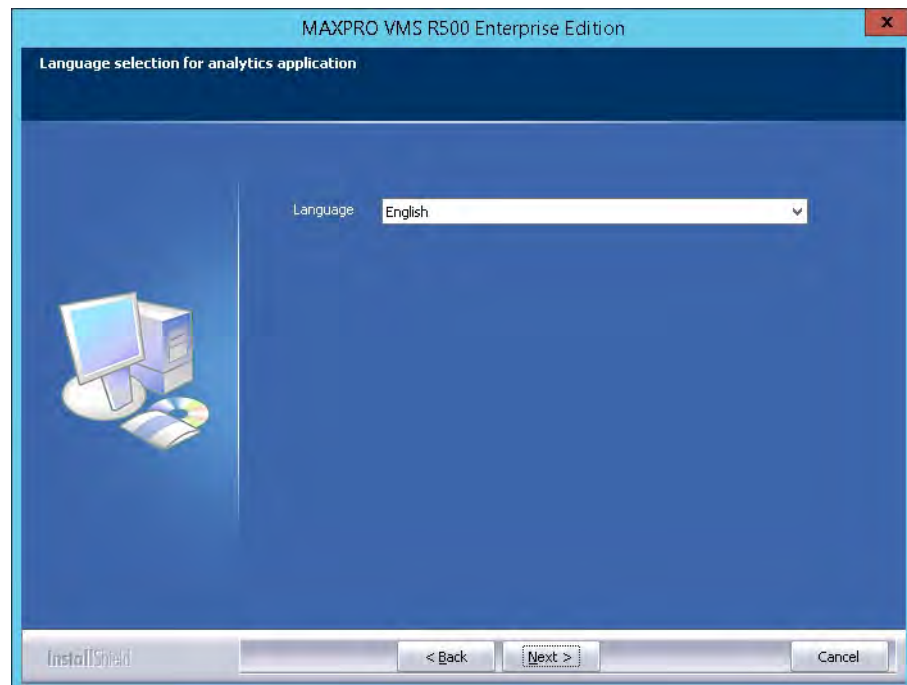


Figure 6-11 Language Selection

14. Select the Language from the drop-down list. Click Next, the Start Copying Files page appears.

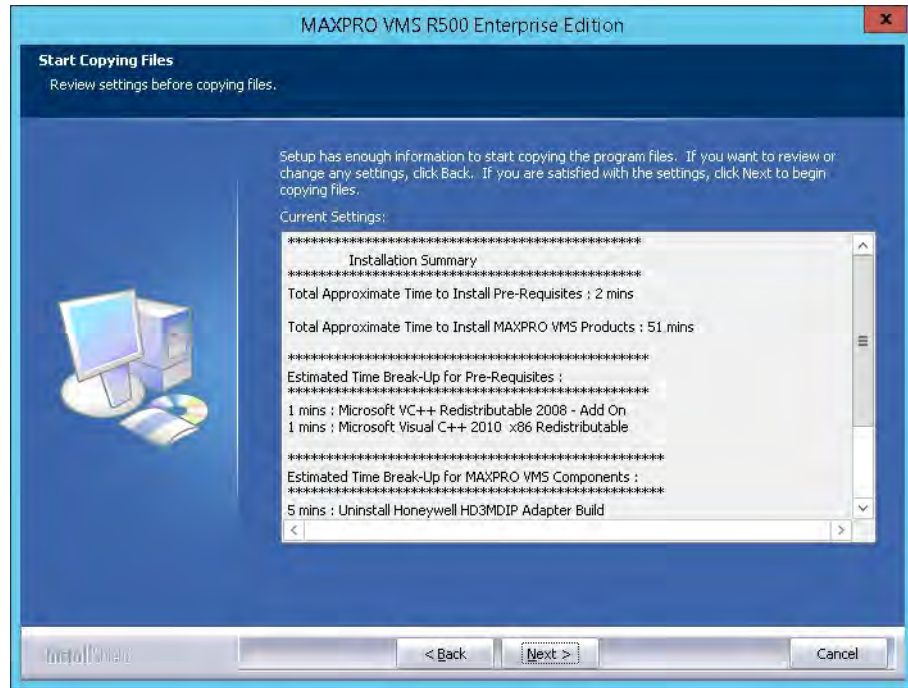


Figure 6-12 Start Copying Files

Note A confirmation message is displayed as shown below. Click **Yes** to proceed and to install the list of prerequisites.

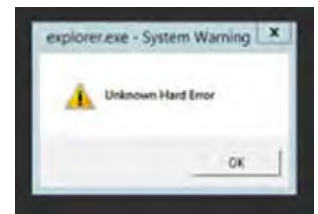


- During Upgrade and when setup is running, a System Warning dialog with Unknown Hard Error message is displayed

Cause: This issue may occur due to conflict between third party applications or due to system file corruption.

Solution: Refer and perform the steps as explained in the following links to solve this issue.

- https://answers.microsoft.com/en-us/windows/forum/windows_8-performance/explorerexe-system-warning-dialog-with-unknown/4c0be311-c9d5-



46e7-b352-c8656f5c0226?auth=1

Or

- <https://www.drivethelife.com/windows-10/fix-unknown-hard-error-windows-10.html>

15. Click Next. The status of various components is displayed. After the components are installed/upgraded successfully, the Upgrade Complete page appears.

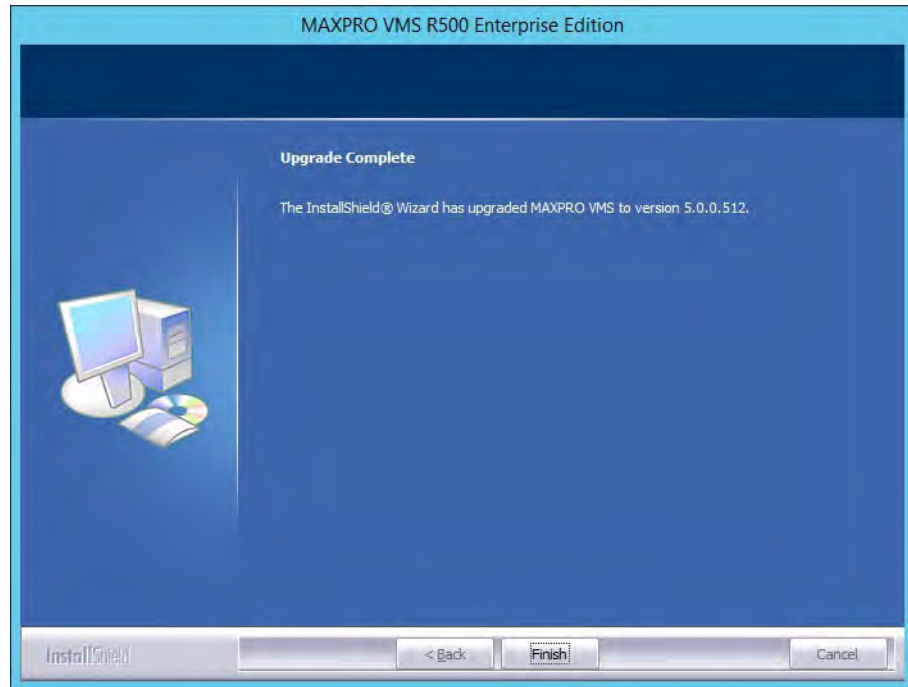


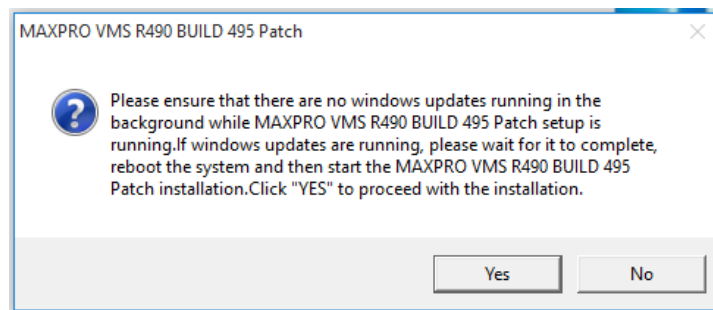
Figure 6-13 Upgrade Complete

16. Click Finish to complete the upgrade.

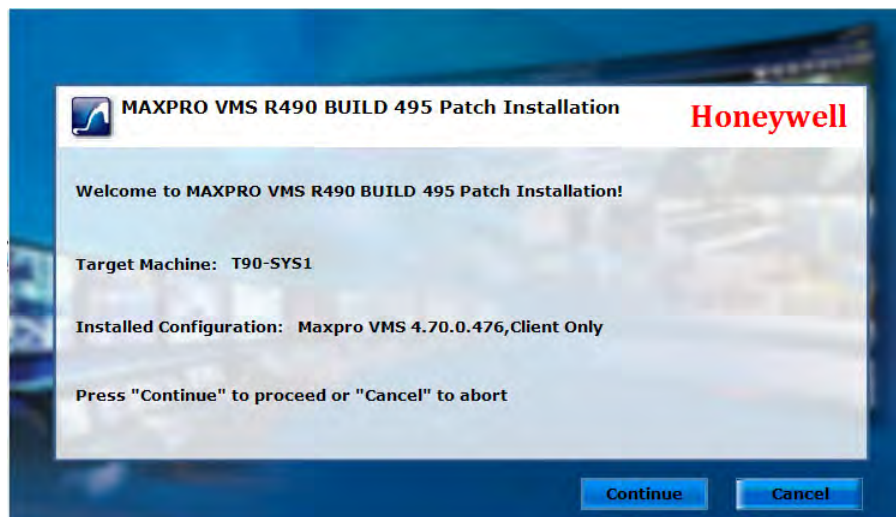
Upgrade MAXPRO VMS R470 Build 476 to R490 Build 495

To upgrade MAXPRO VMS R470 Build 476 to R490 Build 495

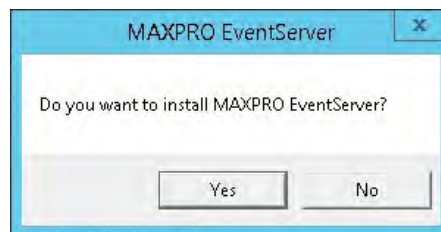
1. Browse to the setup folder and double-click MAXPRO VMS_R490_Build495 Patch Setup. exe. The WinRaR self extracting archive wizard appears and extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



2. Click Yes to disable and proceed. The Welcome page appears.



Note In previous builds if MAXPRO Event Server is not installed then a pop up message to install Event server is displayed as shown below. Click Yes to proceed. See



Upgrade MAXPRO VMS R410 Build 424 to R470 Build 476 section for more information.

3. Click Continue. The installation process continues and once the installation is complete the completion page is displayed as shown below.



4. Click Finish to complete.

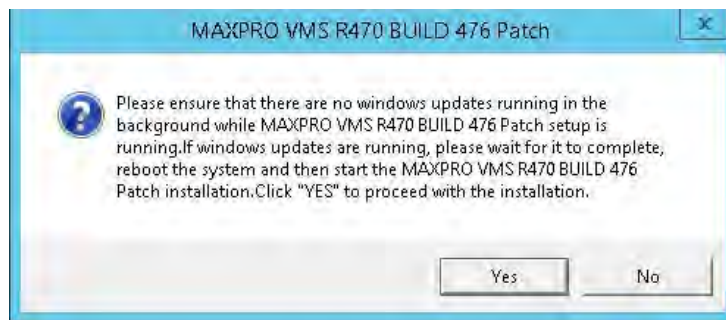
Note If Korean language is not installed in the previous build then a pop up message to install is displayed as shown below. Click Yes to proceed.



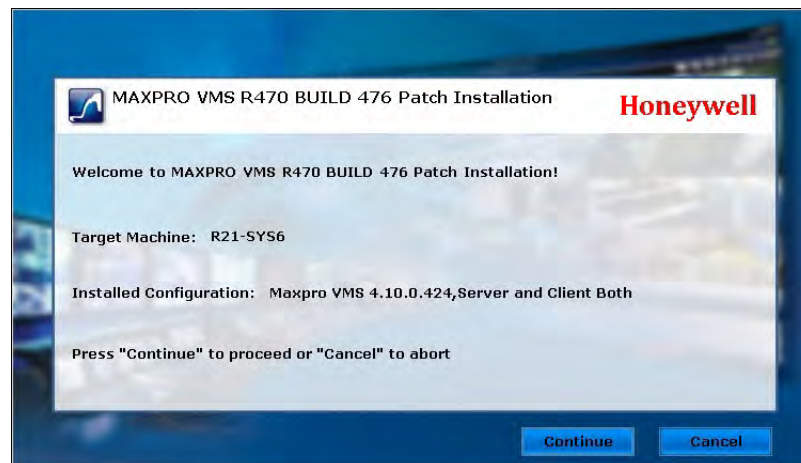
Upgrade MAXPRO VMS R410 Build 424 to R470 Build 476

To upgrade MAXPRO VMS R410 Build 455 to R470 Build 476

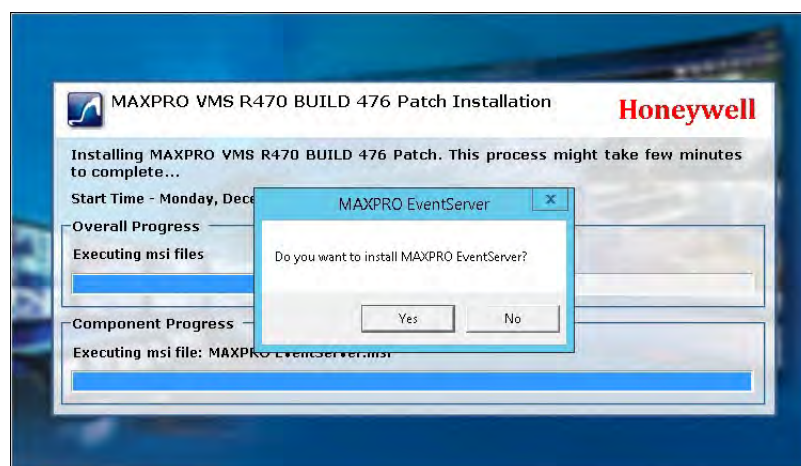
1. Browse to the setup folder and double-click MAXPRO VMS_R470_Build476 Patch Setup. exe. The WinRaR self extracting archive wizard appears and extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



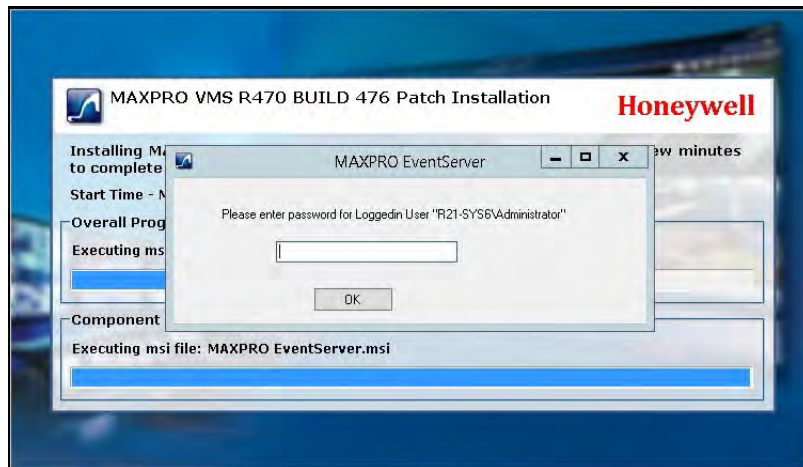
2. Click Yes to disable and proceed. The Welcome page appears.



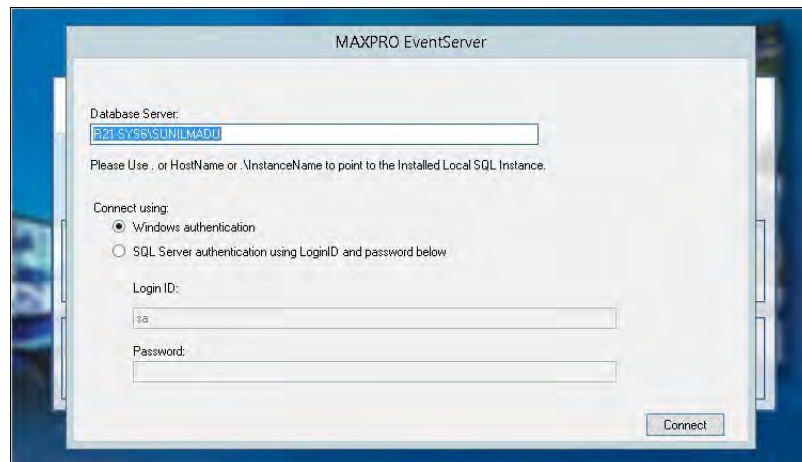
3. Click Continue to start the installation. A confirmation message to install MAXPRO Event Server is displayed as shown below.



- Click Yes. The MAXPRO Event Server authentication box appears as shown below.

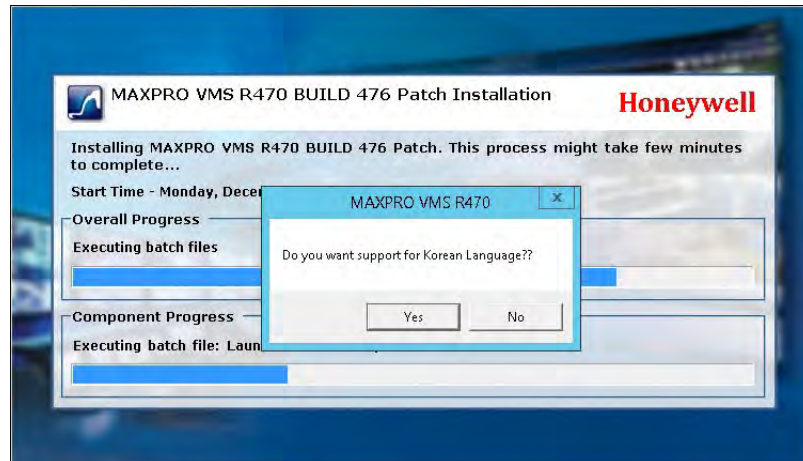


- Type the password for the machine where event server should be installed and then click OK. The Event Server Database details screen appears.



- In Database Server field, type the HostName or InstanceName of the server.
- Select Connect using option as Windows authentication or SQL Server authentication using Login ID and password below as per the requirement. If you connect using the SQL Server authentication then enter the Login ID and Password of the SQL Server installed.

8. Click Connect to continue the installation. A confirmation message to support Korean Language is displayed as shown below.



9. Click Yes if required. The installation process continues and once the installation is complete the completion page is displayed as shown below.

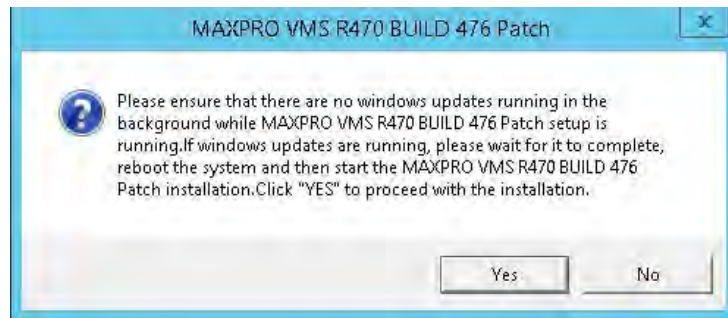


10. Click Finish to complete.

Upgrade MAXPRO VMS R450 Build 455 to R470 Build 476

To upgrade MAXPRO VMS R450 Build 455 to R470 Build 476

1. Browse to the setup folder and double-click MAXPRO VMS_470_Build476 Patch Setup. exe. The WinRaR self extracting archive wizard appears and extracts the setup files. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



2. Click Yes to disable and proceed. The Welcome page appears.



3. Click Continue. The installation process continues and once the installation is complete the completion page is displayed as shown below.

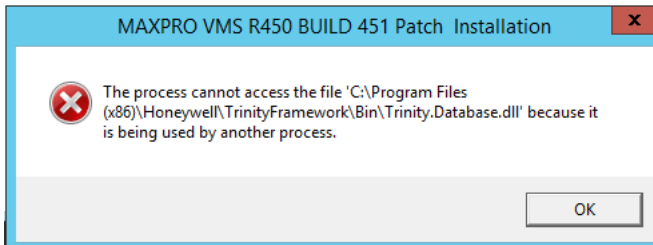


4. Click Finish to complete.

Upgrade MAXPRO VMS R410 Build 424 to R450 Build 455

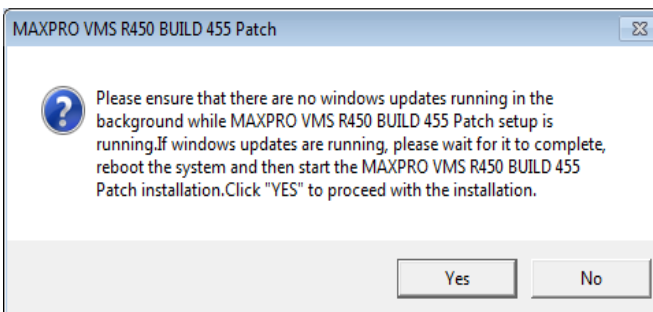
Pre-requisites

Before installing VMS R450 build 455 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.

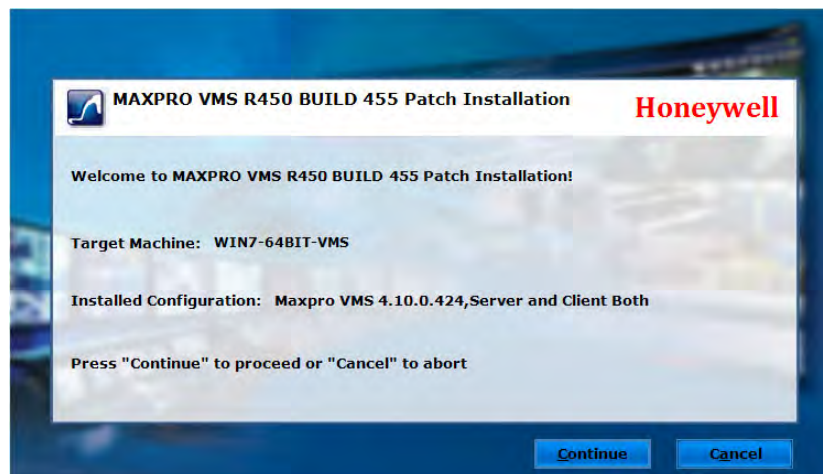


To upgrade MAXPRO VMS R410 Build 424 to R450 Build 455

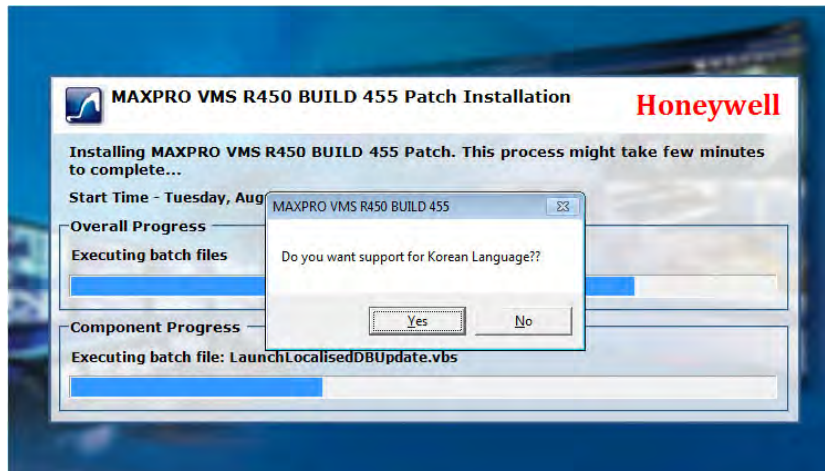
1. Insert the MAXPRO VMS R450 DVD in the DVD drive. The setup runs automatically. If the setup does not run automatically, browse to the setup folder on the DVD and double-click Setup. exe. A confirmation message is displayed to disable the Automatic Windows updates as shown below.



2. Click Yes to disable and proceed. The Welcome page appears.



3. Click Continue to start the installation. A confirmation message to support Korean Language is displayed as shown below.



4. Click Yes if required. The installation process continues and once the installation is complete the completion page is displayed as shown below.

Note: In few machines upgrade process may take more than 20 minutes and this will not effect the patch functionality.



5. Click Finish to complete.

Upgrade VMS R410 Build 424 to R450 Build 455 in Korean OS

MAXPRO VMS R450 Build 455 supports Korean language UI and to upgrade to R450 build 455 in Korean OS, user needs to have R410 Build 424 already installed in the PC.

While installing VMS R410 Build 424 in Korean OS, Installer is not able to proceed due to Trinity database creation issue. To resolve this issue user needs to perform the following task in the order as mentioned.

1. Install the SQL Express_2014 sp1 Database
2. Run the MAXPROVMS_DBUTILITY available as part of setup and also available on Honeywell download center or My Web Tech.
3. Install the R410 Build 424
4. Upgrade to VMS R450 Build 455

Install the SQL Express

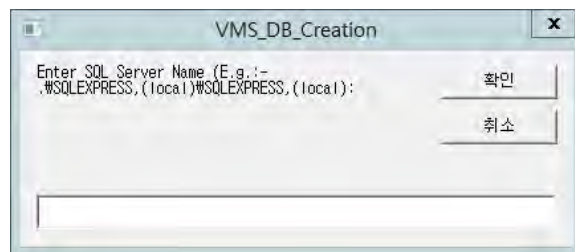
To Install SQL Express_2014 sp1 Database in Korean OS:

1. In VMS installation path, navigate to Raw setup> Prerequisites > SQLExpress2014_SP1 folder.
2. Double -click the SQLEXPRESS_x86_ENU and follow the instructions as explained in SQL installation wizard to complete the installation.

Run the DB Utility

To execute the MAXPROVMS_DBUTILITY in Korean OS:

1. MAXPROVMS_DBUTILITY is part of the R450 B455 setup.exe. Extract the setup.exe Or
Download the MAXPROVMS_DBUTILITY from Honeywell Download center or My Webtech.
2. Double-click the Utility. The VMS_DB_Creation utility is displayed as shown below and prompts you to enter the SQL Instance name as shown below.



3. Type the instance name (For example .\SQLExpress instance name) and then click OK. The installation continues and the utility complete the execution.

Note: Ensure that you provided the same SQLExpress instance name (For example .\SQLExpress instance name) in Database Server Login wizard > Database Server field while installing R410 Build 424.

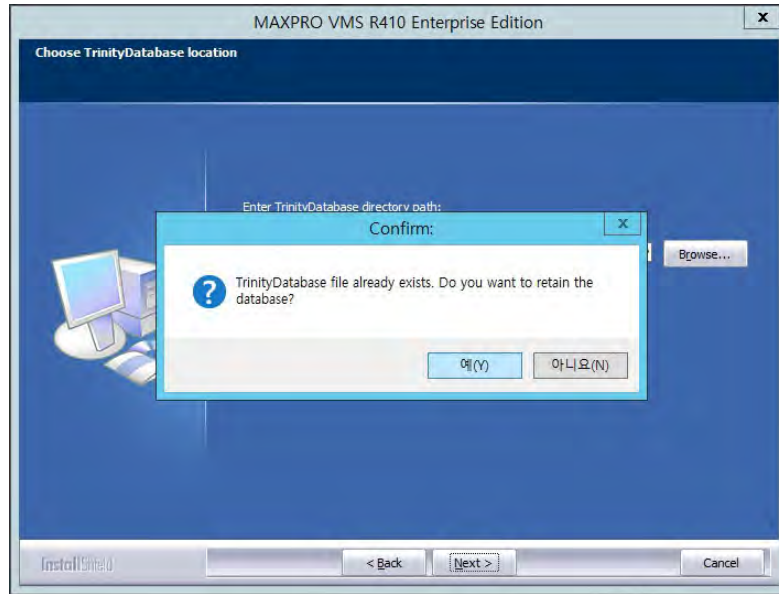
Install VMS R410 Build 424

To install VMS R410 Build 424 in Korean OS:

1. Perform the steps as mentioned in [How to Install MAXPRO™ VMS R670](#) on page [68](#).

Note: Ensure that you type the same SQLExpress instance name which you have created/entered in Step 3 of [Run the DB Utility](#) section.

2. While choosing the Trinity Database Location, a confirm message is displayed to retain the TrinityDatabase as shown below.



3. Ensure that you click Yes to retain the DB and then proceed.

Upgrade to VMS R450 Build 455

- Perform the steps as mentioned in [Upgrade MAXPRO VMS R410 Build 424 to R450 Build 455](#) on page [456](#).

Upgrade to MAXPRO VMS R410

This section describes various scenarios to upgrade the existing version of MAX-PRO VMS to R410 Build 424.

For the following scenarios a common procedure is explained to upgrade MAXPRO VMS software from:

- R300 Build 185 to R310
- R300 Build 188 to R310
- R300 SP1 to R310
- R300 SP2 to R310
- R300 SP2 + 3.5 Driver to R310 Build 326
- R310 Build 326 to R400
- R364 to R400

- B313 + 3.5 NVR driver to R400
- Standalone B313 to R400
- Casino patch 319 to R400
- B301 to R400
- B301 + NVR 3.5 driver to R400
- R310 Build 326 to MAXPRO VMS 410 Build 424

See [Upgrade to MAXPRO VMS R410](#) for more information.

Note: *The upgrade procedure is same for all the patches that are released on top of R300 SP1 and SP2.*

For the below upgrade scenarios, follow the specific procedure mentioned in this chapter.

- R310 Build 313 + 3.5 Driver to R310 Build 326
- R310 Build 301 + 3.5 Driver to R310 Build 326
- R310 Build 323 to R310 Build 326
- R310 Build 326 to MAXPRO_VMS_NVR_4.0_Driver_SP1_Build 364

Before you begin

- Ensure that the client and server computers meet the software requirements.
- User should have .Net 4.6.1 installed on Windows 10 and Windows 2012 OS Machine.

Upgrade to MAXPRO VMS R410

Upgrade MAXPRO VMS R310 to R410 Build 424

See the instructions in the following sections to upgrade to MAXPRO VMS R410 Build 424.

Before you Begin

1. Stop Trinity Services.
 - a. Choose **Start>Run**, and then type **services.msc**. The **Services** window appears.
 - b. Right-click **TrinityController**, and then select **Stop**.
 - c. Right-click **TrinityServer**, and then select **Stop**.
2. Stop the recorder Services if you have any recorder client or server installed.
 - a. Choose **Start>Run**, and then type **services.msc**. The **Services** window appears.

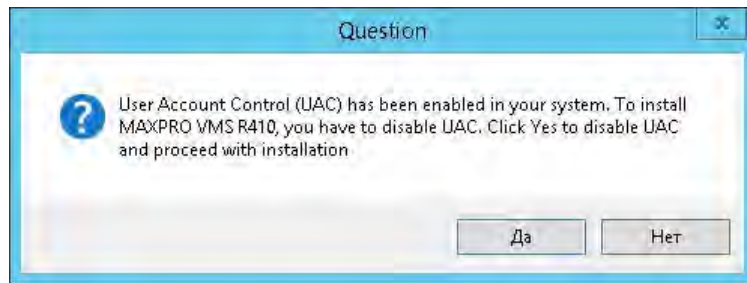
- Caution:** To upgrade recorder driver from MAXPRO VMS R300 to MAXPRO VMS R310, ensure that your computer has Internet Explorer version 7.0 or later.

- ## To upgrade to MAXPRO VMS R410 Build 424

-

-

3. Click Yes to disable and proceed. A UAC message is displayed as shown below.



4. Click Yes to disable the UAC. The Welcome page appears.

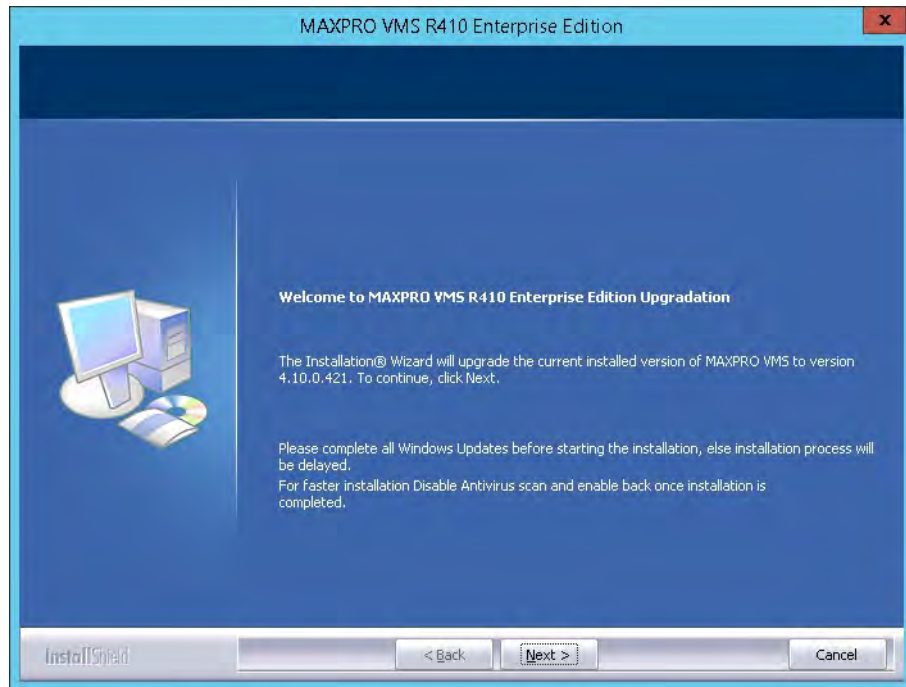


Figure 6-14 Welcome

5. Click Next. The Validation of User Credentials page appears

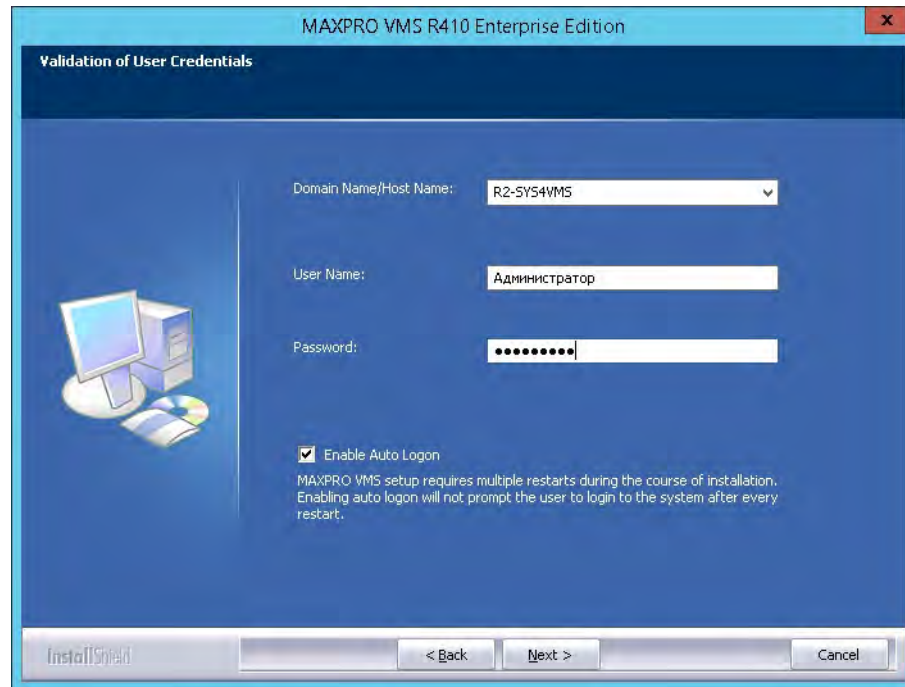
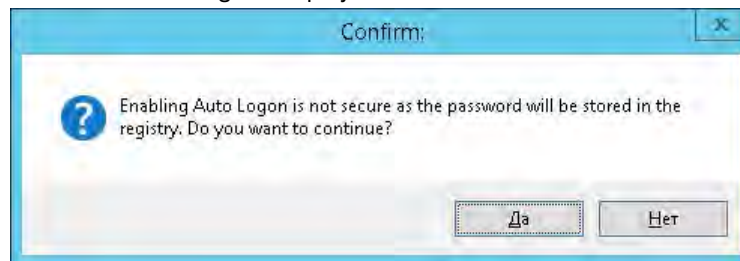


Figure 6-15 Validation of User Credentials

6. In the Domain Name/Host Name list, type the domain name or host name if you know it or select one from the list.
7. In the User Name box, type your Windows user name.
8. In the Password box, type your Windows password.
9. Select the Enable Auto Logon check box if you want the computer to reboot on its own whenever required, during the installation process.

Note You are prompted to reboot multiple times while upgrading to MAXPRO VMS R410, auto log on avoids manual intervention during multiple reboots. A confirmation message is displayed as shown below. Click Yes to continue.



10. Click Next. The Features to be upgraded page appears.

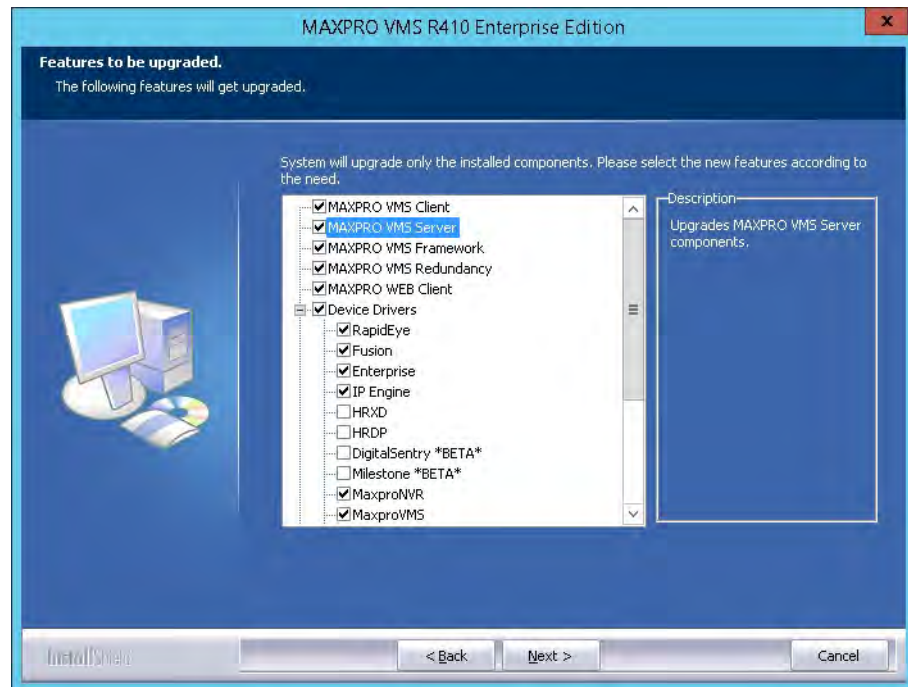


Figure 6-16 Features to be upgraded

11. The check boxes for the features to be upgraded are selected by default. Select the new features you want to install by clicking the respective check boxes.

Note:

- Clear the check boxes for the features that you do not want to install/upgrade.
 - While upgrading the recorder driver, the message “Are you sure you want to remove the Kinley Client” appears. Click **OK** to proceed with the recorder 400.3 upgrade installation.
-

12. Click Next. The Choose Cache file location page appears.

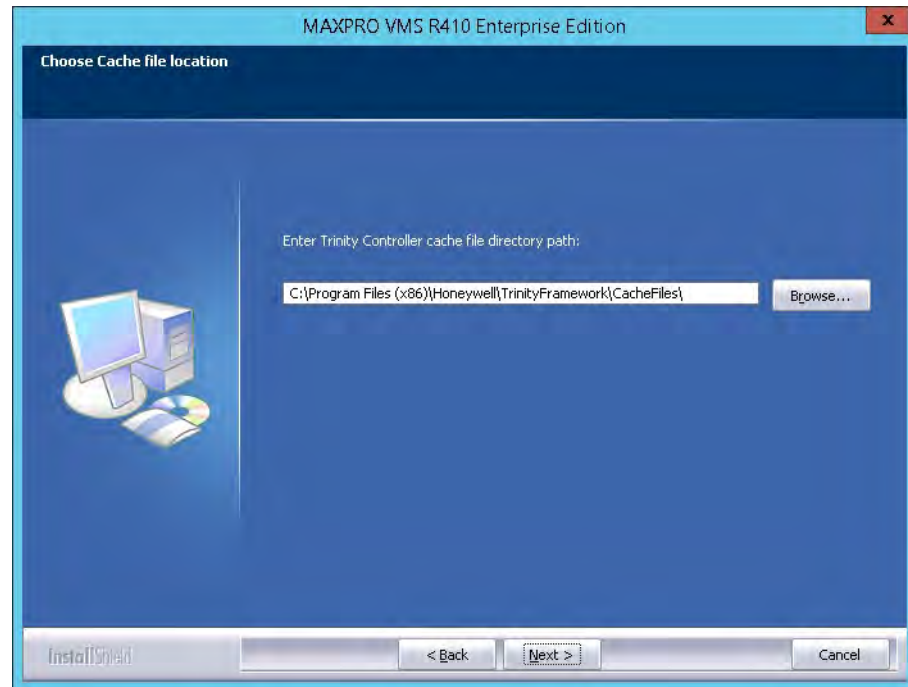


Figure 6-17 Choose Cache File Location

13. Click Next. The Language selection for analytics application page appears.

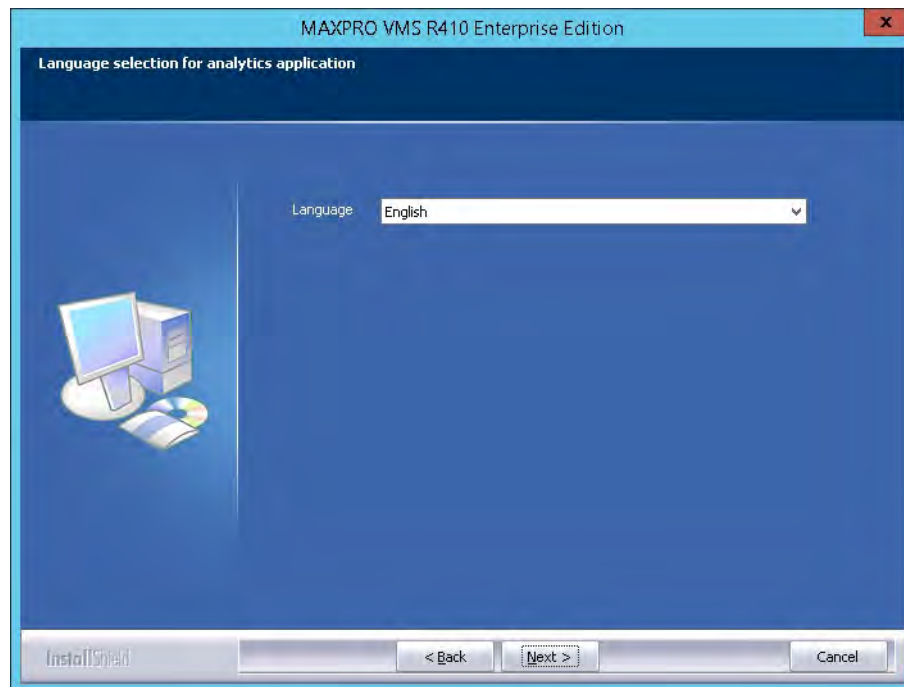


Figure 6-18 Language Selection

14. Select the Language from the drop-down list. Click Next, the Start Copying Files page appears.

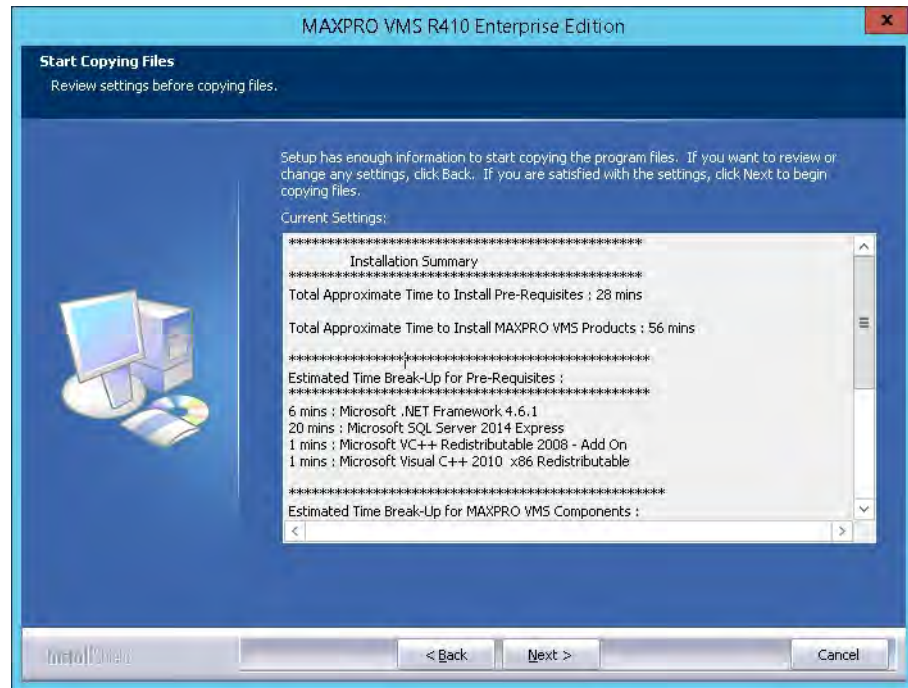


Figure 6-19 Start Copying Files

Note A confirmation message is displayed as shown below. Click Yes to proceed and to install the list of prerequisites.



15. Click Next. The status of various components is displayed. After the components are installed/upgraded successfully, the Upgrade Complete page appears.

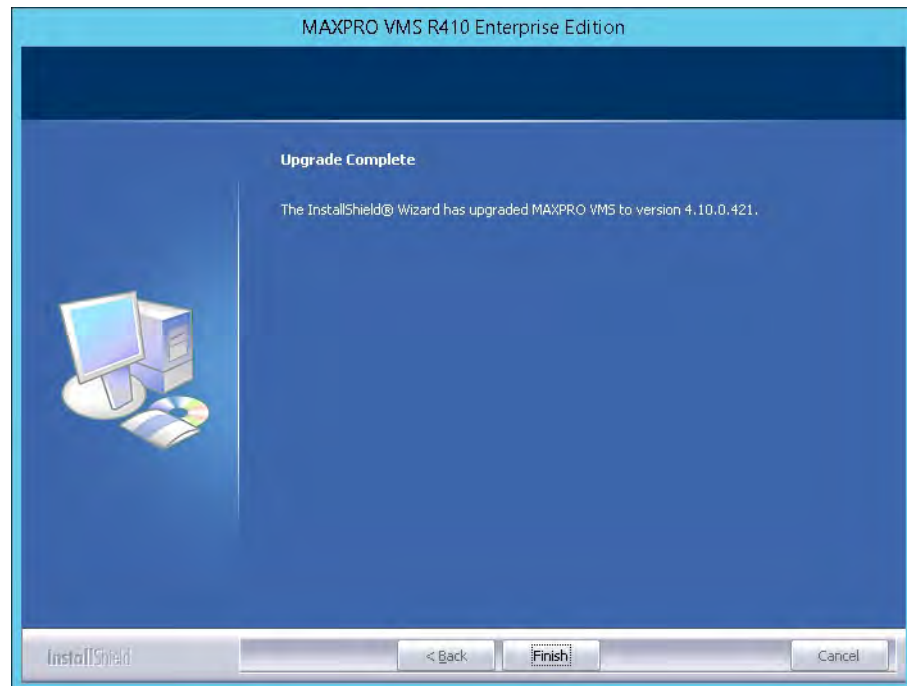


Figure 6-20 Upgrade Complete

16. Click Finish. You are prompted to reboot the computer to complete installation.

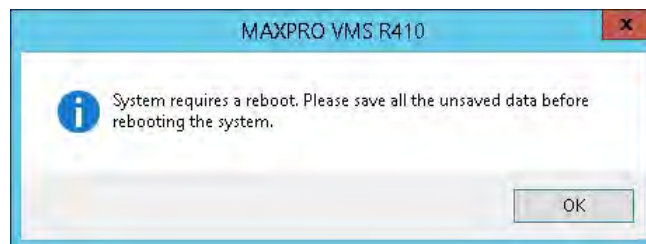


Figure 6-21 Prompt for Rebooting

17. Click OK.

Upgrade MAXPRO VMS R240 To R300

Refer to [MAXPRO® VMS Installation and Configuration Guide](#) to upgrade VMS R240 To MAXPRO VMS R300.

Upgrade VMS R310 B313 with 3.5 Driver to R310 B326

Before upgrading from MAXPRO VMS R310 Build 313 with 3.5 Driver to R310 Build 326 you need to uninstall the following from the server/client PC:

- MAXPRO VMS R310 Build 313 Patch. See [Step 1- Uninstall the MAXPRO VMS R310 Build 313 Patch](#)

- MAXPRO VMS R300 Build 292. See [Step 2- Uninstall the MAXPRO VMS R310 Build 292](#)

After uninstalling the above two patches you can install the MAXPRO VMS R310 Build 326. See [How to Install MAXPRO™ VMS R670](#) on page 68 for more information.

Step 1- Uninstall the MAXPRO VMS R310 Build 313 Patch

1. Navigate to Control Panel > Programs > Programs and Features and then double-click MAXPRO VMS R310 Build 313 Patch.
Or Browse to the setup folder and double-click Setup. exe. The Welcome screen is displayed as shown below.



Figure 6-22 Welcome screen

2. Click Continue. The uninstallation process begins and then uninstall successful screen is displayed as shown below.



Figure 6-23 Uninstallation Completed

3. Click Finish.

Step 2- Uninstall the MAXPRO VMS R310 Build 292

1. Navigate to Control Panel > Programs > Programs and Features and then double-click MAXPRO VMS R310 Build 292.
Or Browse to the setup folder and double-click Setup. exe. The Setup Type page appears.

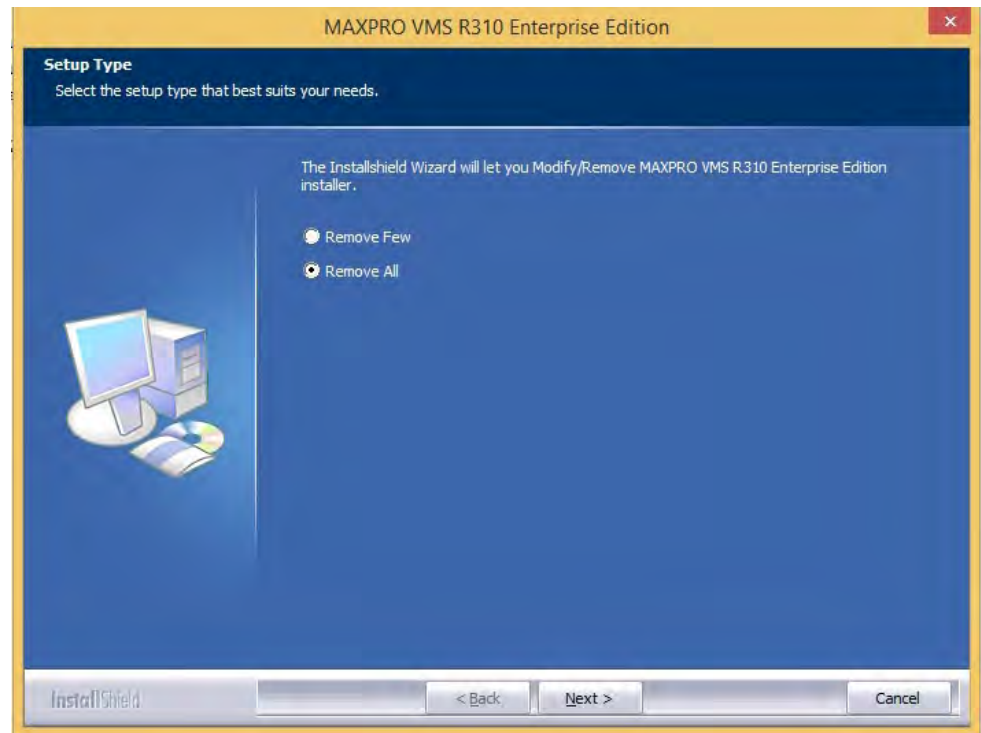
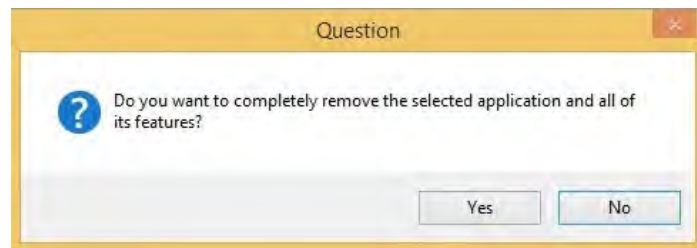
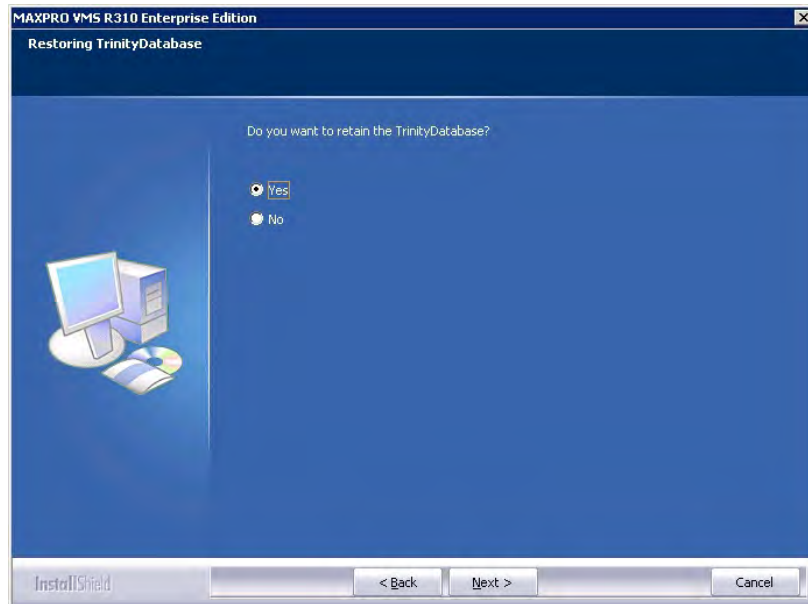


Figure 6-24 Setup Wizard

2. Click the required option to Remove Few or Remove All. A confirmation message is displayed as shown below.



Note If you are uninstalling the build in **Server** machine then **Do you want to retain the Trinity Database?** message is displayed as shown below. Click **Yes** and then click **Next**.



-
3. Click Yes and then click Next. The MAXPRO VMS R310 Build 292 is removed completely and Uninstall Complete page appears.
 4. Click Finish.

Step 3- Install the MAXPRO VMS R310 Build 326

See [How to Install MAXPRO™ VMS R670](#) on page 68 for more information.

Note: While installing MAXPRO VMS R310 Build 326 Server Installation, you are prompted to select the existing database in Database Server login screen. Select Local from the Database Server drop-down to select the Trinity Database which is retained while uninstalling Build 292 in [Step 2- Uninstall the MAXPRO VMS R310 Build 292](#).

Upgrade VMS R310 B 301 with 3.5 Driver to R310 B326

Perform the following steps:

1. Navigate to Control Panel > Programs > Programs and Features and then double-click MAXPRO VMS R310 Build 301.
Or Browse to the setup folder and double-click Setup. exe. The Setup Type page appears.
2. Repeat the step 2 to step 4 as explained in [Step 2- Uninstall the MAXPRO VMS R310 Build 292](#) to uninstall Build 301.

3. Install the MAXPRO VMS R310 Build 326. See [How to Install MAXPRO™ VMS R670](#) on page [68](#) for more information.

Upgrade VMS R310 B 323 to R310 B326

Perform the following steps:

1. Navigate to Control Panel > Programs > Programs and Features and then double-click MAXPRO VMS R310 Build 326.
Or Browse to the setup folder and double-click Setup.exe. The Setup Type page appears.
2. Repeat the step 2 to step 4 as explained in [Step 2- Uninstall the MAXPRO VMS R310 Build 292](#) to uninstall Build 323.
3. Install the MAXPRO VMS R310 Build 326. See [How to Install MAXPRO™ VMS R670](#) on page [68](#) for more information.

Upgrade VMS R310 B326 to NVR 4.0 Driver SP1 B 364

1. Browse to the setup folder and double-click MAXPRO_VMS_NVR_4.0_Driver_SP1_Build364.WinRaR. The WinRaR self extracting archive wizard appears and extracts the setup files. The MAXPRO VMS Device Drivers-InstallShield Wizard appears as shown below.



2. Click Yes to continue. The Installer configure the Device driver setup and displays the Installation wizard.



Figure 6-25 Install Wizard SP1

3. Click Next. The Custom Setup wizard appears and allows you to select the program features to install.

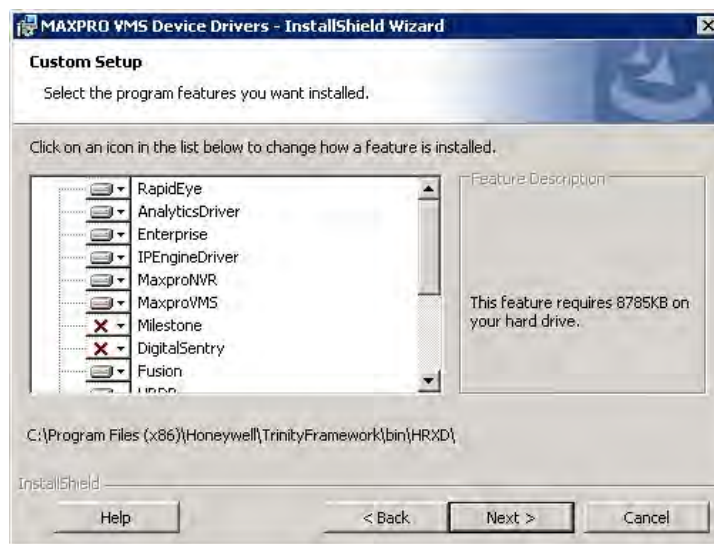


Figure 6-26 Feature Selection

4. Select the required features and then click Next. The Ready to install the Program wizard appears.

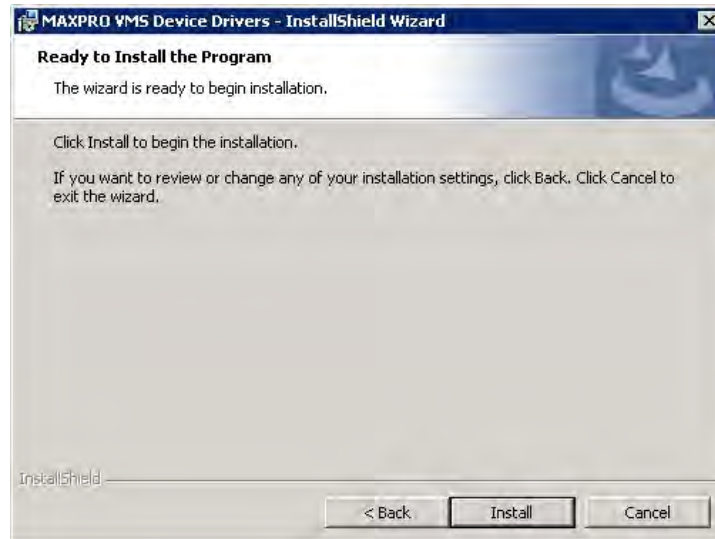


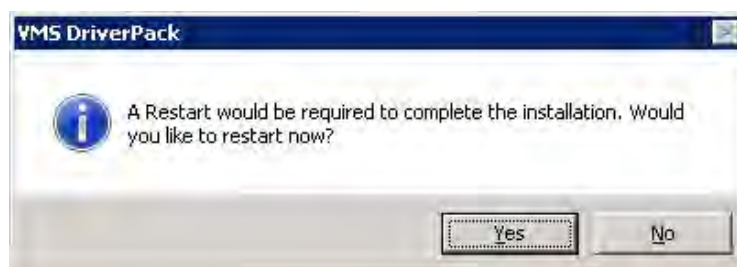
Figure 6-27 Ready to install

5. Click Install. The wizard installs the 4.0 driver. After the components are installed successfully, the Install Complete page appears



Figure 6-28 Install complete

6. Click Finish. You are prompted to reboot the computer to complete installation.



7. Click Yes. After the system reboot, check whether the correct MAXPRO VMS version details is updated with MAXPRO VMS R310 B364 in About window.

This page is intentionally left blank

Introduction

The MAXPRO VMS Web Client allows you to remotely access the MAXPRO VMS 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 VMS Web client is available with MAXPRO VMS 600 along with the VMS 600 installation. You can use the web client once you have installed the VMS 600

MAXPRO VMS Web Client functions involve the following tasks:

- Viewing the live video
- Viewing Recorded Video (Playback)
- Taking Snapshot
- Viewing Presets

Limitation with Privacy Protection Settings

- Anonymization is not supported in Web. If user is tries to see Anonymized video and also camera Anonymized option is enabled then an error message “Trying to access Anonymized Stream” is displayed.
- When an Operator (non-admin) logs into the Web Client and tries to view playback for any video then an error message “Four Eye authentication Privilege Failure” is displayed.

Installing Web Client

During MAXPRO VMS 600 installation, you need to select the Web Client check box in the Select Features wizard and the Web Client component is installed 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 VMS Server using Web Client remotely through a supported web browser then you should install Silverlight on the remote machine.

Prerequisites to access MAXPRO VMS Server through Web Client

The following are the prerequisites to access the MAXPRO VMS server through Web Client.

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

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

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

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

Note MAXPRO VMS 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
-

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

- Web Browsers Supported on MAC systems: Ensure that Safari version 7 or above is installed on your MAC machine.

Setting the MAXPRO Web Configurator

By default MAXPRO VMS installs the Web Configurator and  is displayed on your desktop.

MAXPRO 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 VMS 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.

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

To set the Web Configurator

1. Double-click  on the desktop. The MAXPRO Web Configurator page [figure 1](#) appears. By default the System Configuration tab is selected.

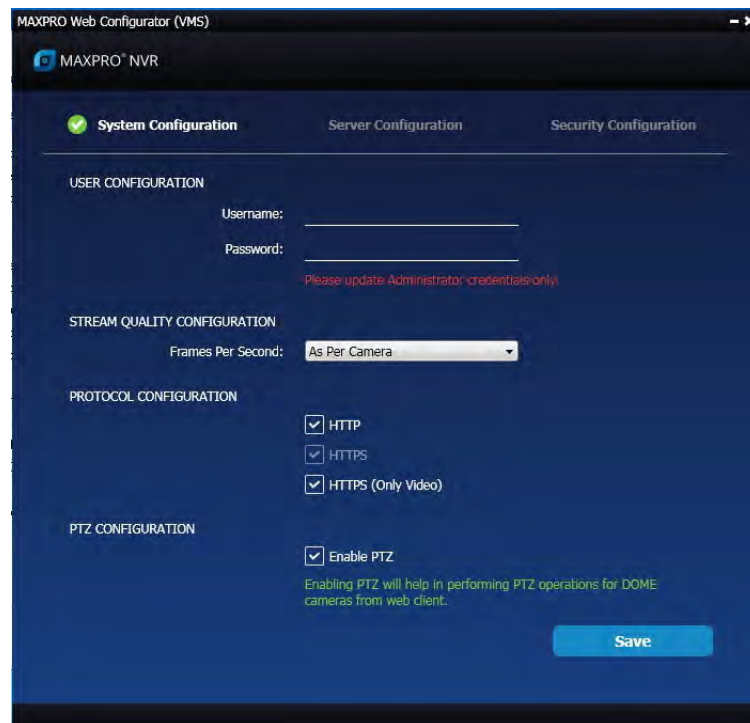


Figure 7-1 System Configuration

2. Under User Configuration: When the (non-window) Administrator log on name and password is changed then you can update the credentials of MAXPRO VMS Web Client to log on.

- Type the Username and Password and then click Update.

Note: You can update only the VMSAdministrator credentials used by the Web Server. If you are changing the default administrator user credentials (admin/trinity) in VMS through the desktop client, then you should change and update the credentials in MaxproWEBConfigurator as well for Web Server to communicate with VMS and Web Clients.

The Administrator credentials used by the Web Server should be configured as a non-Windows Administrator user in the MAXPRO VMS through the desktop client. As a good security practice, it is recommended to update the default credentials on your system.

3. 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 VMS 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 mega-pixel resolutions (above 1080p) then a message appears and video is not displayed as shown below.



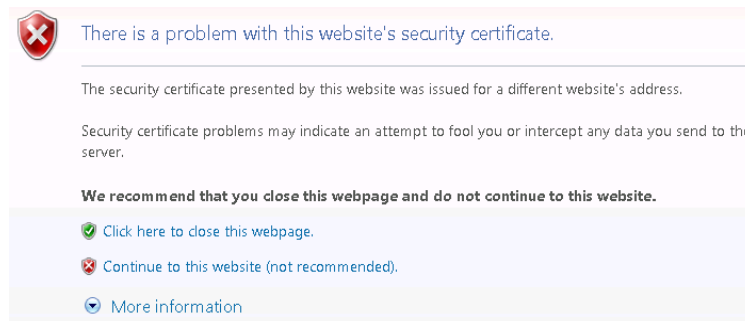
4. Under Protocol Configuration:

- Click the appropriate Protocol options for secure communication. The available options are HTTP, HTTPS and HTTPS (Only Video). 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 VMS server using the URL `https://<MAXPRO VMS Server IP or Machine /Computer name>/MAXPROWEB/` then the following message is displayed. Click Continue to this website to proceed. It is recommended to verify the certificate to check whether it is issued by a valid Certificate Authority. See [Viewing the Certificate Information](#) for more information.



The above message appears by default when you access the VMS server for the first time. Honeywell recommends you to buy a Domain Name specific certificate, create it and then install it. 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.

The above settings are applicable to Internet Explorer, Chrome, Firefox and Safari web browsers. These settings are valid if the web client is accessed using the Domain/Host Name. If you access the web client using the IP then the above settings are not valid.

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

5. Under PTZ Configuration:

- Select the Enable PTZ check box to perform PTZ operations on a PTZ camera from Web Client. Enable PTZ will help in performing PTZ operations for DOME camera from Web Client

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

6. Click Save

7. Click the Server Configuration tab. The Server Configuration screen (figure 2) appears.

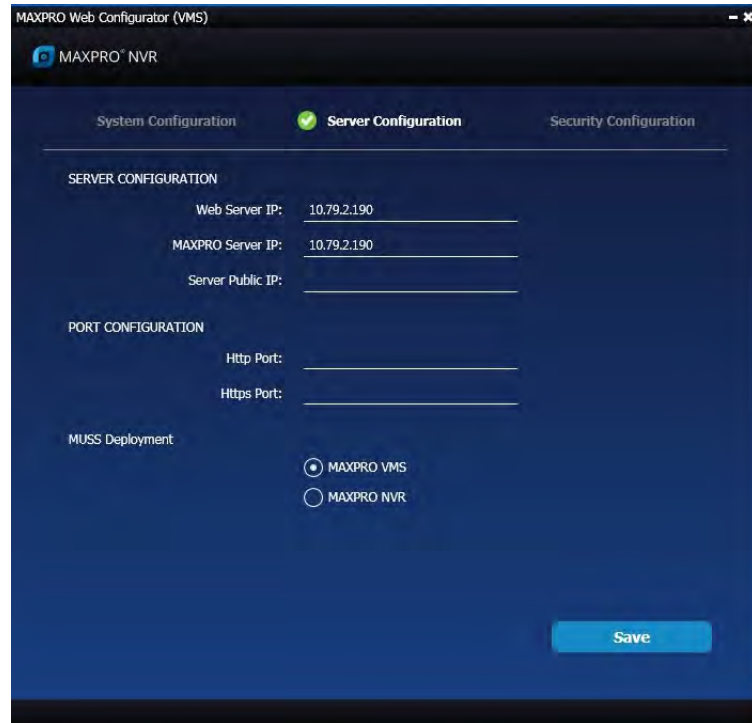


Figure 7-2 Server Configuration

Note: By default the Web Server and the MAXPRO Server is installed on the VMS 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 VMS Server (local) computer/machine name. For Honeywell supplied VMS boxes, default computer/machine name is MAXPRO-VMS and can be updated in the configuration from the tool.

8. Under Server Configuration:

- Web Server IP: If the MAXPRO VMS 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.
- MAXPRO Server IP: If the MAXPRO VMS 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. 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.

9. Under Port Configuration:

- Http Port: If you want to change the http default port 80 to some other port number then type the required port number and click Apply.

- **Https Port:** If you want to change the https default port 443 to some other port number then type the required port number and click Apply.
Port change option in the configurator tool is available from 3.1 Build 65 Rev C or higher version.
10. Under MUSS Deployment, click the MAXPRO VMS or NVR option to deploy.
 - MAXPRO VMS
 - MAXPRO NVR
 11. Click Save
 12. Click the Security Configuration tab. The Security Configuration screen (figure 2) appears.

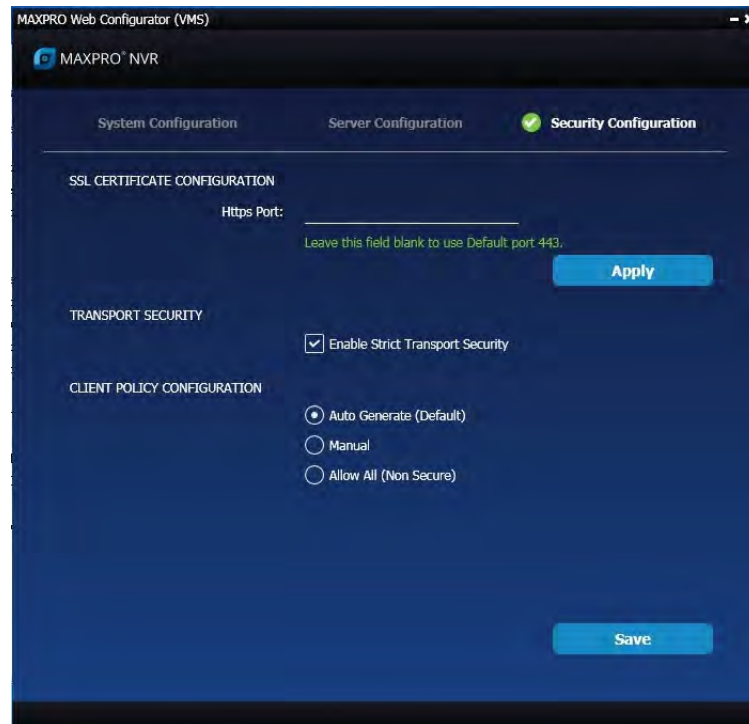


Figure 7-3 Security Configuration

13. Under Self SSL Certificate Configuration:
 - Type the Port number in the box provided if the Https binding is other than 443. The default port is 443 and then click Apply.
14. Under Transport Security, select the Enable Strict Transport Security check box to avoid or protect from hacking.
15. Under Client Policy Configuration: 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](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.**

16. Click Save.

Changing Default Port 443 for Web Client and 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 VMS.
2. Changing the port in the MAXPRO Mobile app and MAXPRO Web Client.

Note: *MAXPRO VMS 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 VMS

By default, Port 443 is configured for the MAXPRO Web Client and MAXPRO Mobile app to connect to the VMS. 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 page appears. By default the System Configuration tab is selected.
2. Click the Server Configuration tab the following screen appears [figure 4](#).

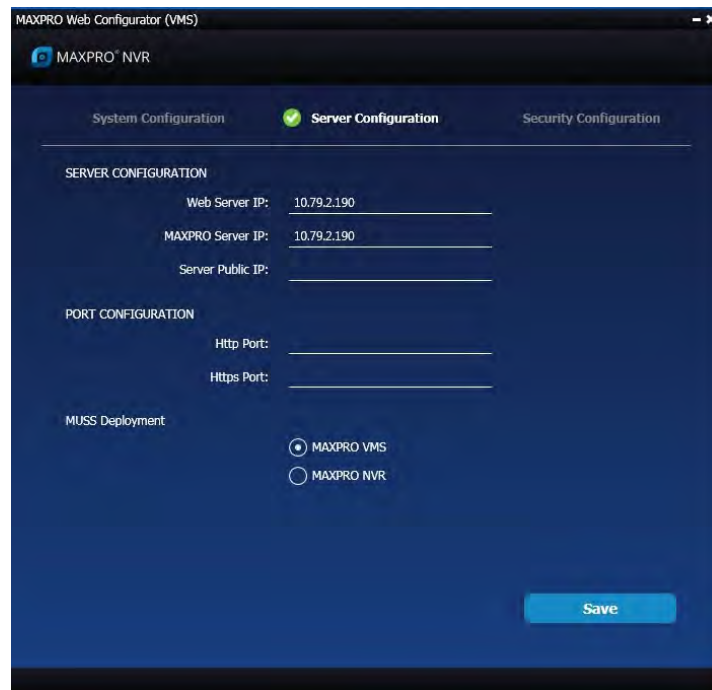



Figure 7-4 Server Configuration

3. Under Port Configuration:
 - Http Port: If you want to change the http default port 80 to some other port number then type the required port number and click Apply.
 - Https Port: If you want to change the https default port 443 to some other port number then type the required port number and click Apply.

Note: Port change option in the configurator tool is available from 3.1 Build 65 Rev C or higher version.

Step 2: Changing the Port in the MAXPRO Web Client and MAXPRO Mobile app

1. Launch MAXPRO Mobile by tapping  on your mobile device.
2. Before you log on: Tap + in the right hand side to add VMS
3. Add the MAXPRO VMS 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 VMS.
 - 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 VMS Web Client:

- Type the URL `https://<MAXPRO VMS Server IP or Computer/Machine name>:<PORT>/MAXPROWEB/` in your web browser and then press Enter. The log In page appears.

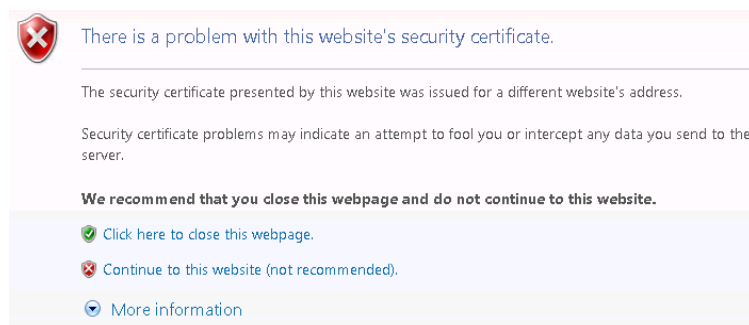
Note: *<MAXPRO VMS Server IP or Computer/Machine name> needs to be replaced by the IP address or Computer/Machine name (as applicable) of the MAXPRO VMS Server machine on which both the Web Server and the VMS Server are installed by default. <PORT> needs to be replaced by the new port. For example: if the port is changed to 1024 with the steps above, enter the URL as `https://74.x.x.x:1024/MAXPROWEB/`*

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

Viewing the Certificate Information

If you see the below security message then it may not be from the valid certificate authority and it would be the case of self signed. It is recommended to exercise caution and verify the certificate and check whether the certificate details are matching with the server machine.

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



To verify the certificate details:

1. Click Continue to this web site (not recommended) link to proceed. The VMS Web Login page is displayed.

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

2. Click Certificate Error as shown below. The Mismatch Address pop up message is displayed.

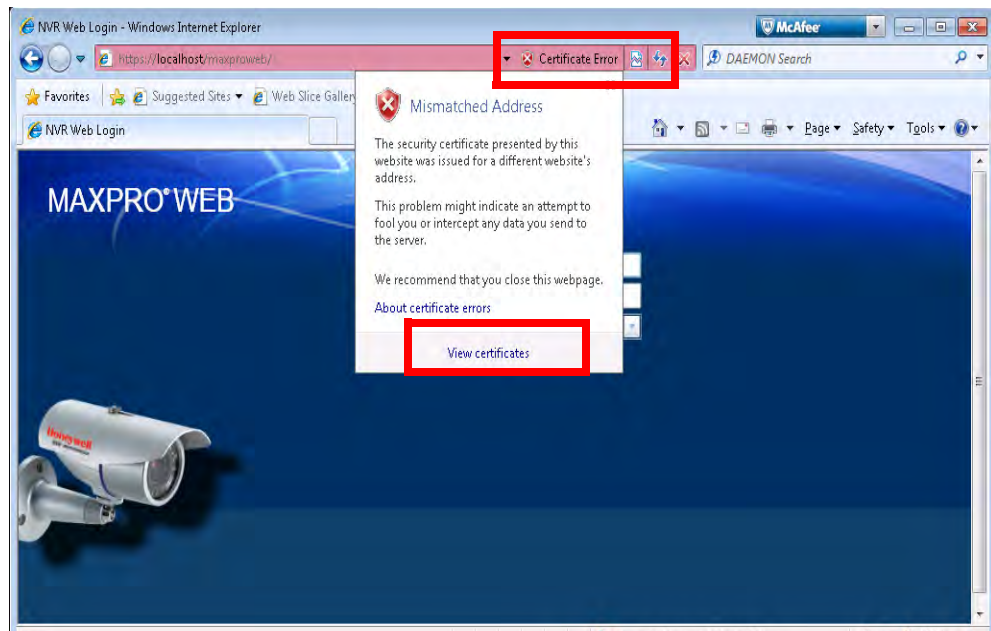


Figure 7-5 Program Maintenance

3. Click View Certificate. The Certificate page is displayed.

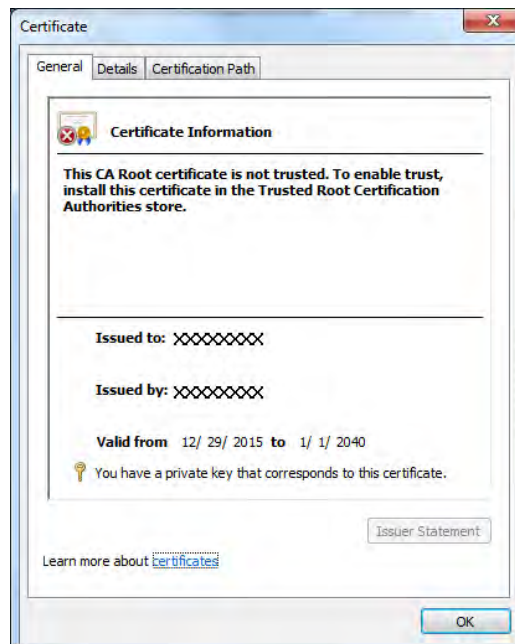


Figure 7-6 Certificate dialog

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.

Honeywell Building Technologies – Security Americas (Head Office)

Honeywell Commercial Security

715 Peachtree St. NE

Atlanta, GA 30308

www.security.honeywell.com/

☎ +1 800 323 4576

Honeywell Building Technologies – Security Mexico

Mexico: Av. Santa Fe 94, Torre A, Piso 1, Col. Zedec,

CP 0121, CDMX, Mexico.

Colombia: Edificio Punto 99, Carrera 11a.

98-50, Piso 7, Bogota, Colombia.

clarsupport@honeywell.com

☎ 01.800.083.59.25

www.honeywell.com

Honeywell Colombia SAS

Carrera 11A # 98-50

Edificio Punto 99, Piso 7, Bogotá DC

Colombia

Honeywell Building Technologies – Security Middle East/N. Africa

Emaar Business Park, Sheikh Zayed Road

Building No. 2, 2nd floor, 201

Post Office Box 232362

Dubai, United Arab Emirates

☎: +971 44541704

www.honeywell.com/security/me

Honeywell Building Technologies – Security Europe/South Africa

Aston Fields Road, Whitehouse Industrial Estate

Runcorn, WA7 3DL,

United Kingdom

www.honeywell.com/security/uk

☎ 08448 000 235

Honeywell Building Technologies – Security Northern Europe

Stationsplein Z-W 961,

1117 CE Schiphol-Oost, Netherlands

www.security.honeywell.com/nl

☎ +31 (0) 299 410 200

Honeywell Building Technologies – Security Deutschland

Johannes-Mauthe-Straße 14 72458 Albstadt, Germany

www.security.honeywell.de

☎ +49 (0) 7431 801-0

Honeywell Building Technologies – Security France

Immeuble Lavoisier

Parc de Haute Technologie 3-7 rue Georges Besse 92160 Antony, France

www.security.honeywell.com/fr

☎ +33 (0) 1 40 96 20 50

Honeywell Building Technologies – Security & Fire (Pacific)

Honeywell Ltd. 9 Columbia Way, BAULKHAM HILLS NSW 2153

Visit: www.honeywellsecurity.com.au, Email: hsf.comms.pacific@Honeywell.com

☎ Tech Support: Australia: 1300 220 345, New Zealand: +64 9 623 5050

Honeywell Building Technologies – Security Italia SpA

Via Achille Grandi 22, 20097 San Donato Milanese (MI), ITALY

www.security.honeywell.com/it

Honeywell Commercial Security - España

Josefa Valcárcel, 24

28027 - Madrid

España

www.honeywell.com

☎ +34 902 667 800

Honeywell Building Technologies – Security Россия и СНГ

121059 Moscow, UI, Kiev 7 Russia

www.security.honeywell.com/ru

☎ +7 (495) 797-93-71

Honeywell Building Technologies – Security Asia Pacific

Building #1, 555 Huanke Road,

Zhang Jiang Hi-Tech Park Pudong New Area,

Shanghai, 201203, China

www.asia.security.honeywell.com

☎ 400 840 2233

Honeywell Building Technologies – Security and Fire (ASEAN)

Honeywell International Sdn Bhd

Level 25, UOA Corp Tower, Lobby B

Avenue 10, The Vertical, Bangsar South City

59200, Kuala Lumpur, Malaysia

Visit Partner Connect: www.partnerconnect.honeywell.com

Email: buildings.asean@honeywell.com

Technical support (Small & Medium Business):

Vietnam: ☎ +84 4 4458 3369

Thailand: ☎ +66 2 0182439

Indonesia: ☎ +62 21 2188 9000

Malaysia: ☎ +60 3 7624 1530

Singapore: ☎ +65 3158 6830

Philippines: ☎ +63 2 231 3380

Honeywell Home and Building Technologies (India)

HBT India Buildings

Unitech Trade Centre, 5th Floor,

Sector – 43, Block C, Sushant Lok Phase – 1,

Gurgaon – 122002, Haryana, India

Visit Partner Connect: www.partnerconnect.honeywell.com

Email: HBT-IndiaBuildings@honeywell.com

Toll Free No: 1-800-103-0339

☎ +91 124 4975000

Honeywell Building Technologies – Security and Fire (Korea)

Honeywell Co., Ltd. (Korea)

5F SangAm IT Tower,

434, Worldcup Buk-ro, Mapo-gu,

Seoul 03922, Korea

Visit: <http://www.honeywell.com>

Email: info.security@honeywell.com

Customer support: HSG-CS-KR@honeywell.com; +82 1522-8779

☎ +82-2-799-6114



Document: 800-26007-C - MAXPRO®VMS R670 Installation and Configuration Guide – 2/2021

www.honeywell.com/security

+1 800 323 4576 (North America only)

<https://honeywellsystems.com/ss/techsupp/index.html>

www.honeywell.com/security/uk

+44 (0) 1928 754 028 (Europe only)

<https://honeywellsystems.com/ss/techsupp/index.html>