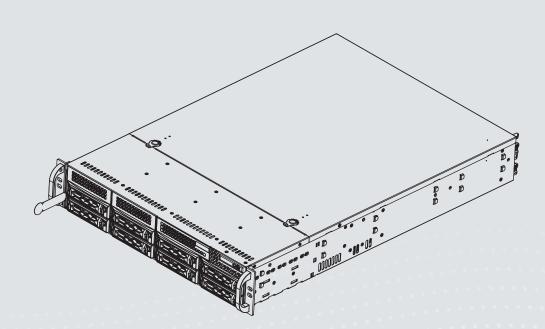


NR9581-v2 NR9681-v2 Network Video Recorder User's Manual

Rack-mount Enclosure • 32-/64-channel Recording • 8x Hot-swappable H.D.D. RAID storage • Full Integration with VIVOTEK Cameras



Rev. 1.0 for VAST rev. 2.9

Table of Contents

Revision History	4
Chapter One Hardware Installation and Initial Configuration	6
Introduction	6
Special Features	6
Safety	7
Installation Instructions	8
Power Supply	9
Environmental Specifications	9
Grounding Requirements	
Physical Description	11
Drive Bay Numbering Sequence	11
Front View	11
Rear View	14
Display	15
Chassis Dimensions	
Rack-mounting	17
Installing Hard Disk Drives	23
Connecting Interfaces	
Initial Configuration	
RAID Basics	
Chapter Two VAST2 Software Configuration and Management	61
Log in	61
Introducing VAST2	
Charged Add-on Features	
Installation Option - OpenVPN	
Chapter 2-1 Basics: Control and Elements	
Hot Keys	
View Cell Elements	
VAST Server and Client Components	
Minimum System Requirements	
Chapter 2-2 Starting Up	100
2-2-1. Selecting Devices	101
2-2-2. Recording Options	102
Seamless Recording	106
Activity Adaptive Stream	107
Adding NAS (Network Attached Storage) as a Storage Option	108
2-2-3. Storage	112
2-2-4. Starting Up - Main Page	113
2-2-5. Saving a View	116
2-2-6. Add More Live Views	117
2-2-7. Save Your Preferences	118
2-2-8. Customizable Layout	119
2-2-9. Dashboard	121

	2-2-10. E-Map	. 123
PI	acing DI/DO Devices	. 126
С	onfiguring Google Map and GPS	. 127
	2-2-11. Event Search	. 133
	2-2-12. PTZ Control	. 136
	2-2-13. Playback	. 138
	2-2-14. Alarm	. 145
	Group Alarm	. 154
	2-2-15. Search Panel	. 158
	2-2-16. Smart search	. 161
	2-2-17. Tour	. 171
	2-2-18. Thumbnail search	. 173
	Chapter 3 Applications:	. 175
	3-1. I/O DI/DO Devices: IO Box and Related Configuration	. 175
	Configuring I/O Box DI/DO as a Trigger or Action in Alarm	. 177
	3-2. Configuring Redundant Servers - Failover	. 181
	Failover Configuration Process	. 188
	3-3. VCA (Video Content Analysis)	
	3-4. VAST Software License	
	Updating Licenses for VAST on Virtual Machines	
	Reminders for VAST Software License	
	Chapter 4 Settings:	
	4-1. Settings > System > Preferences	. 216
	4-2. Settings > Device > Cameras	
	Streaming URL	
	4-3. Logical Folders	
	4-4. Settings > Recording > Recording Options	
	4-5. Settings > Recording > Backup	
	Storage	
	4-6. Settings > Device > Sites	
	Multicasting	
	4-7. Settings > Device > POS	
	4-8. Settings > Device > Local DB	
	4-9. Settings > System > SMTP	
	4-10. Settings > IO Box and Related Configuration	
	Add a New User Account - Windows AD Account	
	Appendix A: VAST Service Control Tool	
	Appendix A: VAST Service Control Tool	
	Appendix D: Mains	
	Appendix C: Joystick Support	
	Appendix E: Using LPR Related Functions w/ Data Magnet	
	Appendix E: Enable Smart Tracking for Speed Dome Cameras	
	Appendix G: Database Merge Function	

Revision History

Rev. 1.0: Initial release. The description for the software functionality is based on VAST rev. 2.9.

WARNING:

- 1. Do not format or initialize the Disk 0: drive on your NVR. The Disk 0: drive contains the operating system. Doing so will disable the system.
- 2. No storage system is completely fail-safe. Damage to data might occur due to file system corruption, operating system malfunction, virus infection, HDD component failures, and so on. Therefore, it is highly recommended to regularly back up your data, and VIVOTEK disclaims responsibilities of data loss or recovery.
- 3. Always power off the system using the power down button on system desktop. Do not disconnect the power cord while the system is still operating. Doing so will result in data inconsistencies. The normal power-off procedure allows cached data to be written to disks.

Some low quality Ethernet cables with smaller core diameter can seriously reduce the transmission rate. Use CAT5e or CAT6 cables with a wire gauge of 24AWG for NVR's uplink port. A thicker core 24 AWG network cable can offer less resistance than a 26 AWG or 28 AWG network cable.

Use shielded cables in high noise environments where cross talk and EMI can occur.

Technology License Notice



Notices from HEVC Advance:

THIS PRODUCT IS SOLD WITH A LIMITED LICENSE AND IS AUTHORIZED TO BE USED ONLY IN CONNECTION WITH HEVC CONTENT THAT MEETS EACH OF THE THREE FOLLOWING QUALIFICATIONS: (1) HEVC CONTENT ONLY FOR PERSONAL USE; (2) HEVC CONTENT THAT IS NOT OFFERED FOR SALE; AND (3) HEVC CONTENT THAT IS CREATED BY THE OWNER OF THE PRODUCT. THIS PRODUCT MAY NOT BE USED IN CONNECTION WITH HEVC ENCODED CONTENT CREATED BY A THIRD PARTY, WHICH THE USER HAS ORDERED OR PURCHASED FROM A THIRD PARTY, UNLESS THE USER IS SEPARATELY GRANTED RIGHTS TO USE THE PRODUCT WITH SUCH CONTENT BY A LICENSED SELLER OF THE CONTENT. YOUR USE OF THIS PRODUCT IN CONNECTION WITH HEVC ENCODED CONTENT IS DEEMED ACCEPTANCE OF THE LIMITED AUTHORITY TO USE AS NOTED ABOVE.

Read Before Use

The use of surveillance devices may be prohibited by law in your country. The Network Camera is not only a high-performance web-ready camera but can also be part of a flexible surveillance system. It is the user's responsibility to ensure that the operation of such devices is legal before installing this unit for its intended use.

It is important to first verify that all contents received are complete according to the Package Contents listed below. Take note of the warnings in the Quick Installation Guide before the Network Camera is installed; then carefully read and follow the instructions in the Installation chapter to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

The Network Camera is a network device and its use should be straightforward for those who have basic networking knowledge. It is designed for various applications including video sharing, general security/surveillance, etc. The Configuration chapter suggests ways to best utilize the Network Camera and ensure proper operations. For creative and professional developers, the URL Commands of the Network Camera section serves as a helpful reference to customizing existing homepages or integrating with the current web server.

セキュリティ基準(新規則第34条の10)

「本製品は 電気通信事業者(移動通信会社、固定通信会社、インターネットプロバイダ等) の通信回線(公衆無線LANを含む) に直接接続することができません。本製品をインターネットに接続する場合は、必ずルータ等 を経由し接続してください。」

NOTE:

The operating system and management software are installed on a flash memory mounted on the main board. Except for the plug-ins for onscreen display, there is no need to install software.

Symbols and Statements in this Document



INFORMATION: provides important messages or advices that might help prevent inconvenient or problem situations.



NOTE: Notices provide guidance or advices that are related to the functional integrity of the

Tips: Tips are useful information that helps enhance or facilitae an installation, function, or process.

WARNING! or **IMPORTANT**: These statements indicate situations that can be dangerous or hazardous to the machine or you.

Electrical Hazard: This statement appears when high voltage electrical hazards might occur to an operator.

Chapter One Hardware Installation and Initial Configuration

Introduction

NR9581/9681-v2 is the latest 64- or 32-channel H.265, RAID-protected NVR from VIVOTEK, bringing stable and efficient system operation under a wide range of recording/network management/system settings. The unit supports all VIVOTEK camera models, including the latest 5-Megapixel and fisheye cameras. The support for RAID 1/5/6/10 provides data security in the event of disk drive failure.

The unit is equipped with two gigabit Ethernet RJ45 ports which provide network failover functionality to avoid the risk of recording loss. When one network line is disconnected, the system will shift to the other network automatically, providing continuous access for video data. Up to 8 HDDs can be installed in the NR9581/9681 for a total storage capacity of up to 48TB (6TB max. each). Eight removable HDD trays are available in the front of the unit, with hot-swap functionality for easy replacement.

A VAST2 CMS server runs on the machine that manages surveillance recording and playback. The compatibility with the iViewer application allows for remote access to the NR9581-v2/ NR9681-v2 on handheld devices. By integrating all of the components together using VIVOT-EK's NVR, network cameras, VAST2, and iViewer software, users can realize a fully-featured and robust next-generation surveillance system. This ingenious NVR also features the remote management capability with a full range of server/client structures and thus is capable for robust and diverse applications.

Special Features

- Runs on embedded Windows
- 2U Rack Mount Design
- RAID 0, 1, 5, 6, 10, 50, 60 in virtual drive storage configurations
- 8 x HDD Tray, for a max. capacity of 48TB
- 2 x Gigabit RJ45 Ethernet ports
- 6 x USB Port (2 x Front / 4 x in Back)
- Size: 17.2" (437 mm) (W) x 25.5" (647 mm) (D) x 3.5" (89 mm) (H)
- Gross Weight: 33 lbs (14.97 kg)
- 64-CH Live View & 16-CH Synchronous Playback
- H.265/H.264/ MPEG-4
- PTZ Support
- Snapshot / Export Media
- PiP Video Control
- Bookmark Design
- Fast Configuration Backup / Restore
- Pre-installed VIVOTEK VAST Central Management Software*
- Full Integration with VIVOTEK Network Cameras
- VIVOTEK iViewer Support (iOS/Android)

Safety

- 1. Read these safety instructions carefully.
- 2. Keep this User Manual for later reference.
- 3. Disconnect this equipment from any AC outlet before cleaning. Use a damp cloth. Do not use liquid or spray detergents for cleaning.
- 4. For plug-in equipment, the power outlet socket must be located near the equip-ment and must be easily accessible.
- 5. Keep this equipment away from humidity.
- 6. Put this equipment on a reliable surface during installation. Dropping it or letting it fall may cause damage.
- 7. For rack-mount equipment, please firmly install the device with pallets or sliding rails in the rack.
- 8. Do not leave this equipment in an environment unconditioned where the storage temperature under 0° C (32° F) or above 40° C (104° F), it may damage the equipment.
- 9. The openings on the enclosure are for air convection. Protect the equipment from overheating. DO NOT COVER THE OPENINGS.
- 10. Make sure the voltage of the power source is correct before connecting the equipment to the power outlet.
- 11. Position the power cord so that people cannot step on it. Do not place anything over the power cord.
- 12. All cautions and warnings on the equipment should be noted.
- 13. If the equipment is not used for a long time, disconnect it from the power source to avoid damage by transient overvoltage.
- 14. Never pour any liquid into an opening. This may cause fire or electrical shock.
- 15. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
- 16. If one of the following situations arises, get the equipment checked by service personnel:
 - The power cord or plug is damaged.
 - Liquid has penetrated into the equipment.
 - The equipment has been exposed to moisture.
 - The equipment does not work well, or you cannot get it to work according to the user's manual.
 - The equipment has been dropped and damaged.
 - The equipment has obvious signs of breakage.
- 17. **CAUTION**: The computer is provided with a battery-powered real-time clock circuit. There is a danger of explosion if battery is incorrectly replaced. Replace only with same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.
- 18. This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interferencethat may cause undesired operation.

- 19. **CAUTION**: Always completely disconnect the power cord from your chassis whenever you work with the hardware. Do not make connections while the power is on. Sensitive electronic components can be damaged by sudden power surges.
- 20. **CAUTION**: Always ground yourself to remove any static charge before touching the motherboard, backplane, or add-on cards. Modern electronic devices are very sensitive to static electric charges. As a safety precaution, use a grounding wrist strap at all times. Place all electronic components on a static-dissipative surface or in a static-shielded bag when they are not in the chassis.
- 21. **CAUTION**: Any unverified component could cause unexpected damage. To ensure the correct installation, please always use the components (e.g., screws) provided with the accessory box.

Installation Instructions



Warning:

Read the installation instructions before connecting the system to the power source.



Warning:

This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 250V, 20 A.



Warning:

The system must be disconnected from all sources of power and the power cord.removed from the power supply module(s) before accessing the chassis interior to install or remove system components.



Warning:

Only trained and qualifiedpersonnel should be allowed to install, replace, or service this equipment.



Warning:

This unit is intended for installation in restricted access areas. A restricted access area can be accessed only through the use of a special tool, lock and key, or other means of security. (This warning does not apply to workstations).



Warning:

There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.



Warning:

This unit might have more than one power supply connection. All connections must be removed to de-energize the unit.



Warning:

Hazardous voltage or energy is present on the backplane when the system is operating. Use caution when servicing.



Warning:

Installation of the equipment must comply with local and national electrical codes.



Warning:

Ultimate disposal of this product should be handled according to all national laws and regulations.



Warning:

The fans might still be turning when you remove the fan assembly from the chassis. Keep fingers, screwdrivers, and other objects away from the openings in the fan assembly's housing.



Warning:

When installing the product, use the provided or designated connection cables, power cables and AC adaptors. Using any other cables and adaptors could cause a malfunction or a fire.Electrical Appliance and Material Safety Law prohibits the use of UL or CSA -certified cables (that have UL/CSA shown on the code) for any other electrical devices than products designated by the manufacturer only.

Power Supply

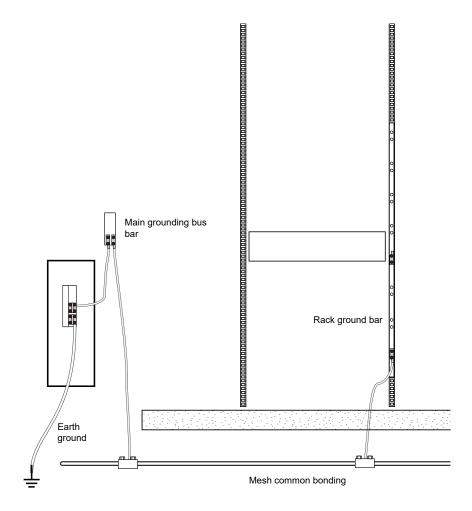
Watt	600W max. (94+ Gold, PFC) (1+1 Redundant 2U)		
Input rating	600W with Input 100 - 127Vac, 50-60Hz		
Output voltage	+12 V: Max: 50A (100Vac - 127Vac); Max: 54.16A (200Vac - 240Vac); Max: 54.16A (200 -		
	240) @ 45A. +5Vsb: Max: 4A / Min: 0A		
Power distributor	PDB-PT826-L8824 - O/P: 12V/75, +5V Max: 30, +3.3V Max: 24, -12V Max: 0.6		
Safety	BSMI/CCC/CE/EMC/FCC		

Environmental Specifications

Environment	Operating	Non-operating
Temperature	5 ~ 35°C (32 ~ 104°F)	40 ~ 70°C (-40 ~ 158°F)
Humidity	8 ~ 90% @ 40°C, non-condensing	5 ~ 95% @ 60°C, non-condensing

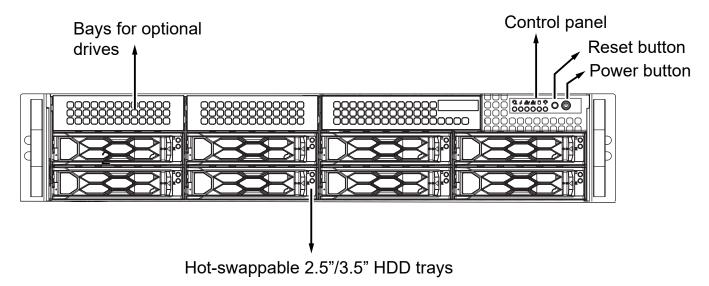
Grounding Requirements

- 1. The enclosure is designed to be rack-mounted, in an equipment room which has limited human access.
- 2. In addition to the grounding via the power cords, make sure your equipment rack is properly grounded.
- 3. Use a ground wire of a copper cross section of at least 16AWG.

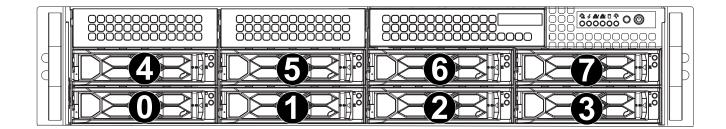


Physical Description

Front View



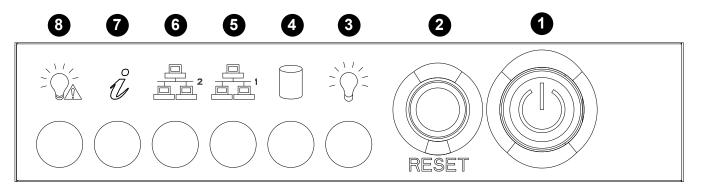
Drive Bay Numbering Sequence





Warning:

Knowing the correct positions of hard drives is very important. For example, if a hard drive fails in a RAID5 Virtual Drive, you can initialize a rebuild by locating and replacing the failed drive. If you replace the wrong drive, it means that you have 1 failed drive and another mistakenly failed drive. Having 2 failed drives in a RAID5 configuration renders all data inaccessible. All data in the RAID5 Virtual Drive will be lost.



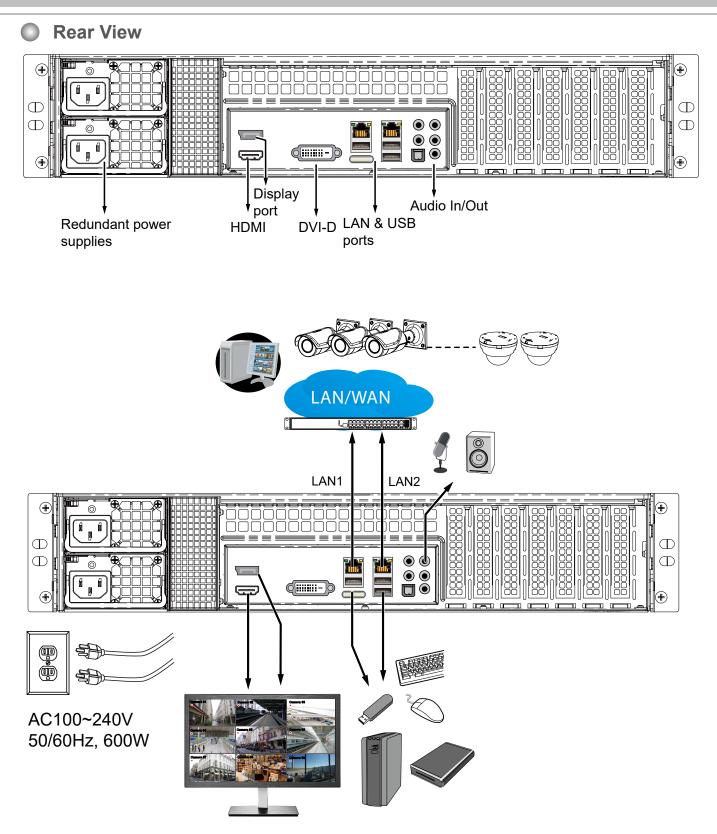
Contro	ol Panel buttons and LEDs		
1 Power switch		Press this switch to turn the system power on or off. Please use system shutdown or press this switch for a few seconds to turn off the system ATX power.	
		The main power switch is used to apply or remove power from the power supplies to the server. Turning off system power using this button removes the main power but keeps standby power supplied to the system. You must unplug the system before servicing components inside the chassis.	
2	Reset button	Press this button to reboot the system.	
3	Power LED	Indicates power is being supplied to the system power supply units. This LED is illuminated when the system is operating normally.	
4	HDD LED	Indicates hard disk drive activities	
5	LAN status LED	Indicates network activity on LAN1 when flashing.	
6	LAN status LED	Indicates network activity on LAN2 when flashing.	
7	Information LED*	Alerts operator to several states, as noted in the table below.	
8	Power failed LED	Indicates a power supply module has failed.	

* The HDD LED here only displays the status for those attached to the motherboard. They do not display the status for the hard disks in the 16 drive bays

Information LED	
Continuously on and red	An overheat condition has occurred. (This may be caused by cable congestion.)
Blinking red (1Hz)	Fan failure, check for an inoperative fan.
Blinking red (0.25Hz)	Power failure, check for a non-operational power supply.
Solid blue	UID has been activated locally to locate the server in a rack environment.
Blinking blue	UID has been activated using IPMI to locate the server in a rack environment.

Each drive carrier has two LED indicators: an activity indicator and a status indicator. For RAID configurations using a controller, the meaning of the status indicator is described in the table below. For OS RAID or non-RAID configurations, some LED indications are not supported, such as hot spare.

Drive Tray LED Defi	nitions		
	Color	Blinking pattern	Device Behavior
Activity LED	Blue	Solid ON	SAS drive installed
		Blinking	I/O activity
Status LED	Red	Solid ON	Failure of drive with RSTe
			support
		Blinking at 1 Hz	Rebuild drive with RSTe
			support
		Blinking with two blinks and	Hot spare for drive
		one stop at 1 Hz	with RSTe support (not
			supported in VMD mode)
		On for five seconds, then	Power on for drive with
		off	RSTe support
		Blinking at 4 Hz	Identify drive with RSTe
			support



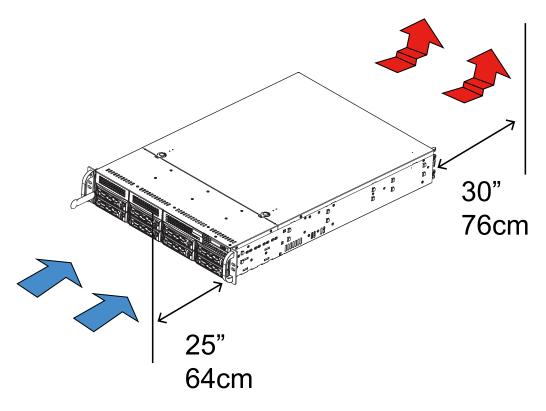
Display

Interface	Resolution
HDMI	Supports max resolution HDMI 1.2 1920 x 1200 @ 60 Hz
DVI-D	Currently not supported. Supports max. resolution 1920 x 1200 @ 60 Hz
Display port	Supports max resolution 4096 x 2304 @ 60 Hz
eDP	Internal pin header, supports max. resolution 3840 x 2160 @ 60 Hz (on board)

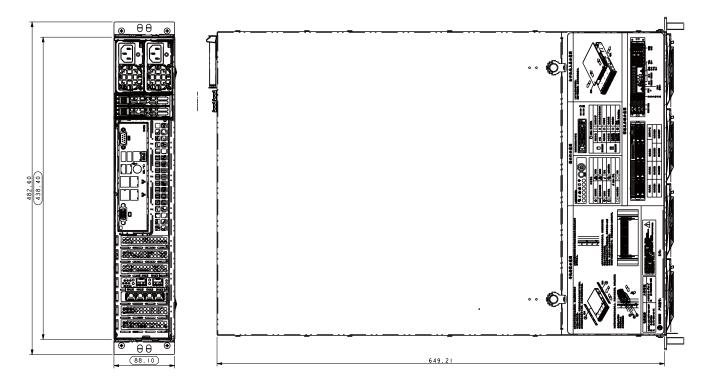
MIMPORTANT:

It is important to leave a clearance of 76cm to the rear side of the chassis. The clearance is required to ensure an adequate airflow through the chassis to ventilate heat. A 64cm clearance is also required on the front of the chassis.

To ensure normal operation, maintain ambient airflow. Do not block the airflow around chassis such as placing the system in a closed cabinet.



Chassis Dimensions



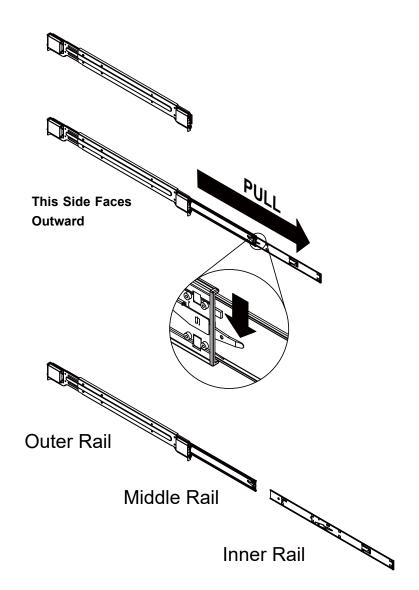
SCALE 1:2

Rack-mounting

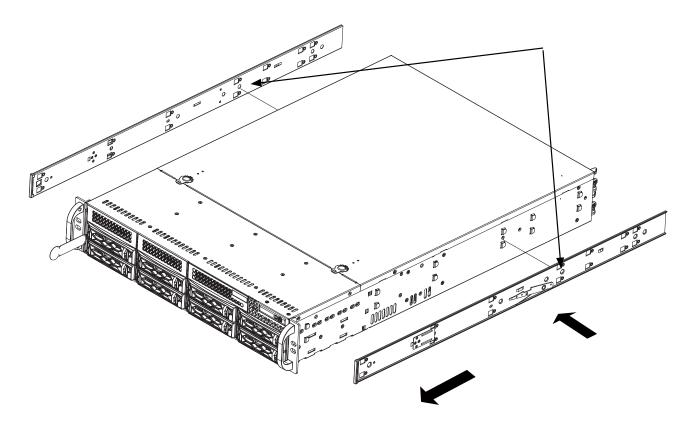
If you have either a round-holed or square-holed rack, install cage nuts or clip nuts to the desired positions on the rack posts.

The instructions below are based on the installation to a 4-post equipment rack.

1. Remove the inner rail from the slide rail assembly. There is a locking tab at the tip of the inner rail.



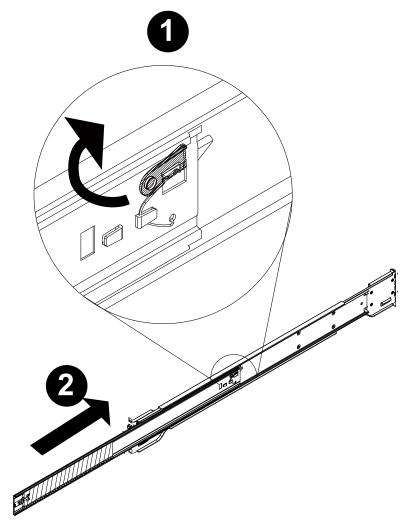
2. Secure the inner rails to the sides of the chassis using the included screws. Place the inner rail firmly against the side of the chassis, aligning the hooks on the side of the chassis with the holes in the inner rail. Slide the inner rail forward toward the front of the chassis and under the hooks until the quick release bracket snaps into place, securing the rail to the chassis.



Do not pick up the server with the front handles. They are designed to pull the system from a rack only.

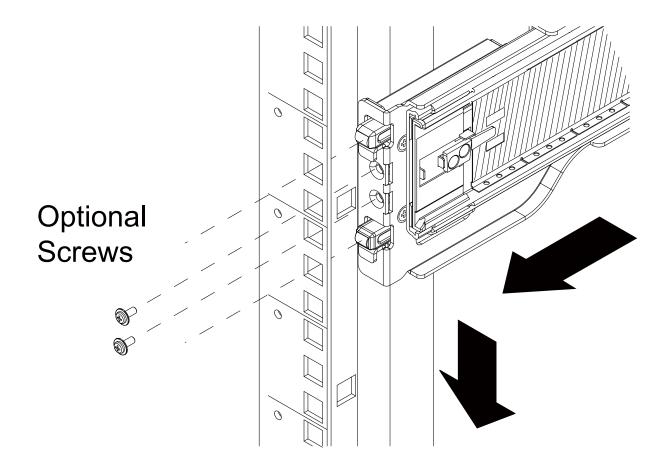
3. Pull upward on the locking tab at the rear end of the middle rail.

Push the middle rail back into the outer rail.



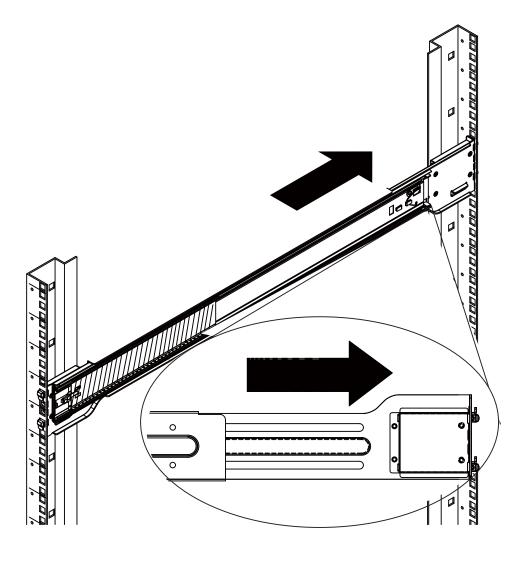
4. Hang the hooks on the front of the outer rail onto the square holes on the front of the rack. If desired, use screws to secure the outer rails to the rack.

It is important to check if the safety lock is in the unlocked position before mounting the brackets.



5. Pull out the rear of the outer rail, adjusting the length until it just fits within the posts of the rack.

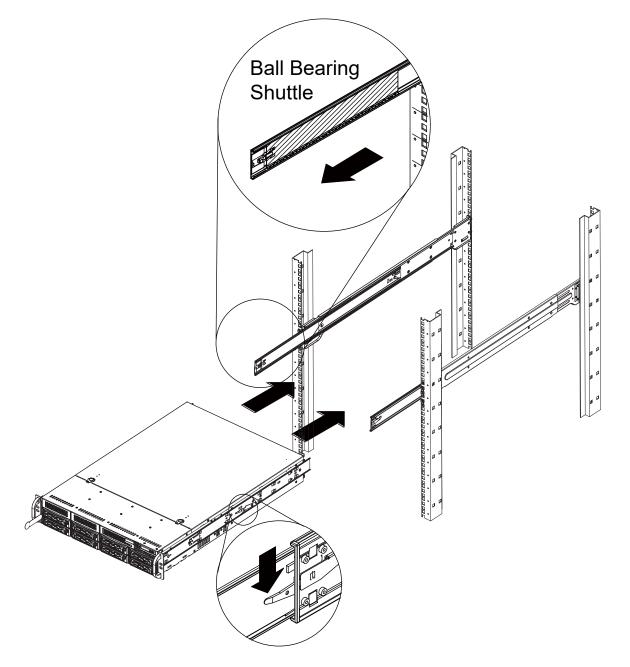
Hang the hooks of the rear section of the outer rail onto the square holes on the rear of the rack. Take care that the proper holes are used so the rails are level. If desired, use screws to secure the rear of the outer rail to the rear of the rack.



6. Pull the middle rail out of the front of the outer rail and make sure that the ball bearing shuttle is locked at the front of the middle rail.

Align the rear of the chassis rails with the middle rails and then push evenly on both sides of the chassis until it clicks into the fully extended position.

Depress the locking tabs on both sides of the chassis and push the it fully into the rack. The locking tabs should "click".



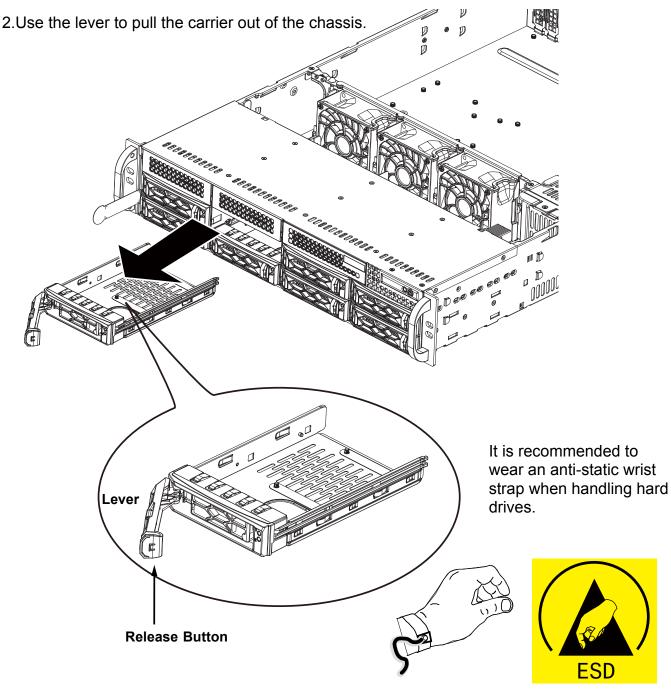
Note: Keep the ball bearing shuttle locked at the front of the middle rail during installation. Note: Figure is for illustrative purposes only. Always install servers to the bottom of a rack first.

Installing Hard Disk Drives

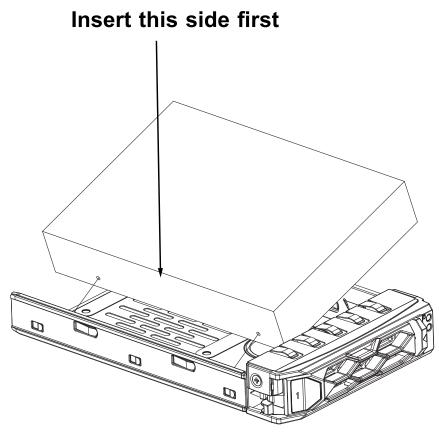


- Refer to VIVOTEK's website for the hard disk compatibility information.
- Avoid touching the hard drive's circuit board or connector pins. Doing so can damage the hard drive by electro-static discharge.

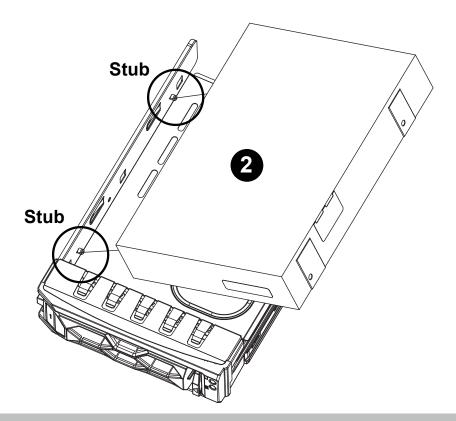
1. Press the release button on the drive carrier. This extends the drive carrier lever.



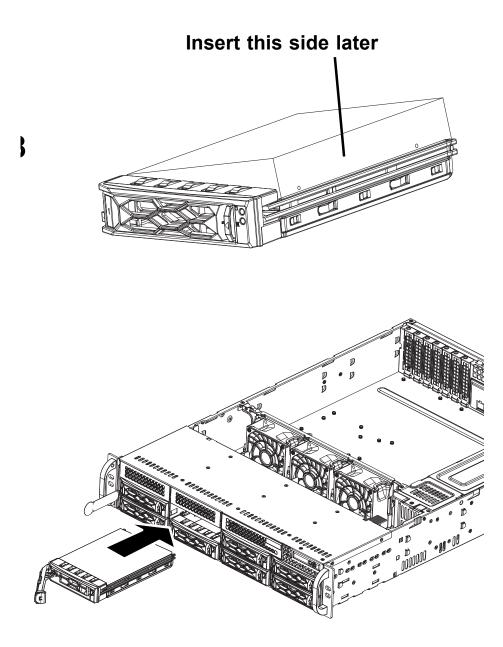
3. Insert a 3.5" hard drive in an angle into the carrier, so that the mounting holes on the right side of the drive align with the two stubs in the drive carrier. Insert this side into the drive carrier first, then push the other side into the drive carrier completely.



3.5" Drive



4. Press down on the other side for the hard drive to snap into place.



If using 2.5" hard drives, the 4 screws necessary for installation are user-supplied.

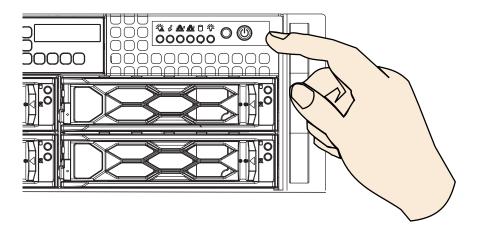
Connecting Interfaces

Refer to page 14 for the interface connections.

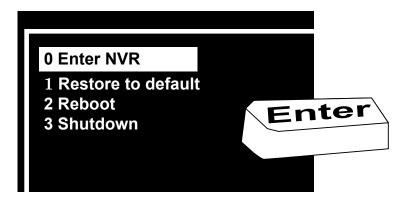
- 1. Make sure all cameras have been properly installed, either they are powered by 12V power lines or using one or several PoE switches or mid-spans. Refer to the cameras' documentation for details.
- 2. Connect all other interfaces to USB mouse/keyboard, one or two monitors, and audio input/ output devices.
- 3. Make sure you connect both power supplies to power mains. An alarm will be sounded if you connect only 1 of the power supplies.

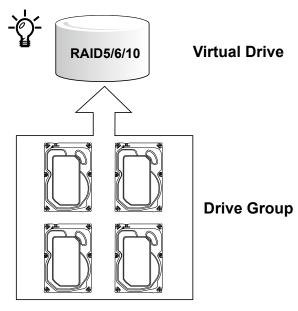
Initial Configuration

1. Power up the system by pressing the power on button.



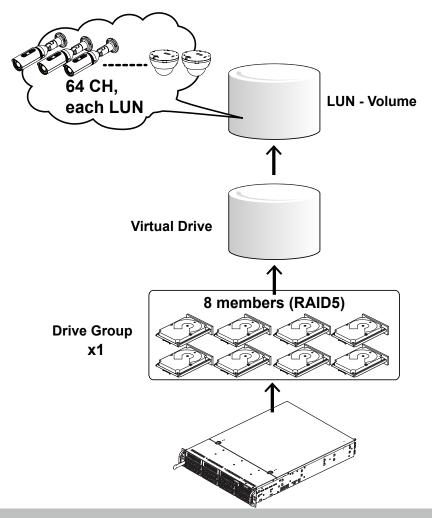
2. Skip the BIOS screens and select **Enter NVR** at the selection screen. The system will start. Wait for the start-up process to complete.





Our default recommendation is to combine 4 hard drives into 1 drive group. The capacities of these drives will be utilized to form 1 Virtual Drive. If all 16 drive bays are populated, you can create 4 Virtual Drives. A 4-member Virtual Drive can receive the video feeds from 32 cameras. You can also create two 8-member Virtual Drives to receive the video feeds from 64 cameras (CH, or channels.)

Recording will not take place unless you create a Virtual Drive first. Select RAID5 as the RAID level during the configuration process.



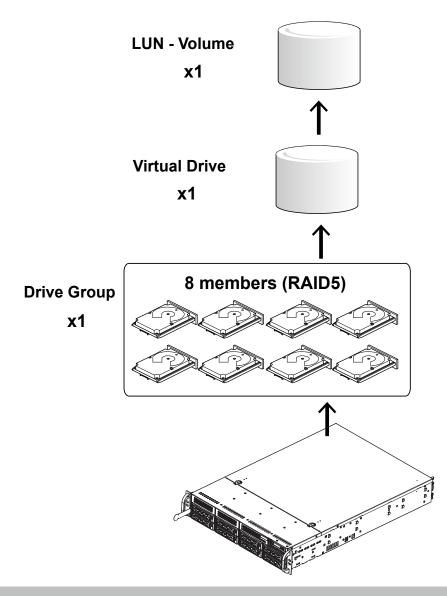
The default configuration for a configuration of 64 cameras should look like the following:

Physical & Logical	Configuration
components	
Hard drive	8
Virtual Drive	1, each has 8 members. Configured in RAID5.
	If using 6TB drives, the available capacity in each Virtual Drive will be, 8 x 6TB-1 x 6TB(parity drive)= 42TB.
Volume	2, each created from 1 Virtual Drive.

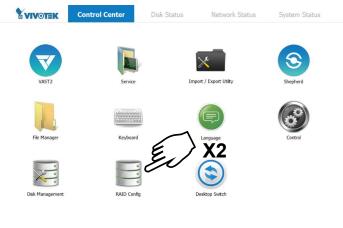
The camera configuration should look like this,

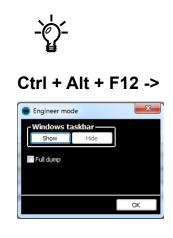
Physical & Logical	Configuration
components	
Cameras	64
Recording Group	1, each responds to 32 or 64 cameras, and each Recording Group is associated with 1
	Virtual Drive volume.
Volume	1, each created from 1 Virtual Drive, and associated with 1 Recording Group.

A Virtual Drive appears to the host system (Windows) as a logical disk partition. The logical parition, when formatted, becomes a disk volume.



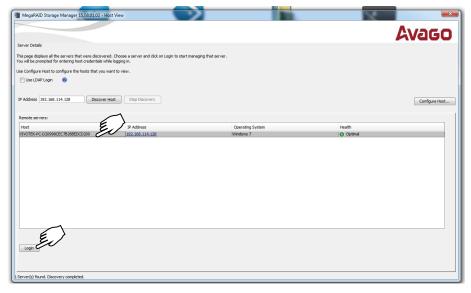
1. The system will boot up to the system main screen. Double-click on the **RAID Config** shortcut to start the MegaRAID storage configuration utility.





0

2. Select the default server, namely, the Windows 7 server running on this machine. Click Login to begin your configuration.



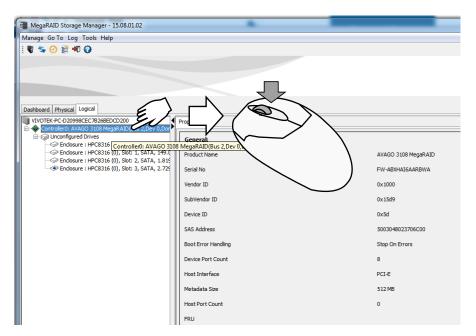
3. Enter vivotek/vivotek as the User Name and Password. Click Login to proceed.

🛢 Enter User Name & P	assword	×
	Ave	GO
Server :	127.0.0.1 Use your Operating System and password to login the rer	0
User Name:	vivotek Defau vivotek vivot	
Password:	vivot	-
Login Mode:	Full Access	

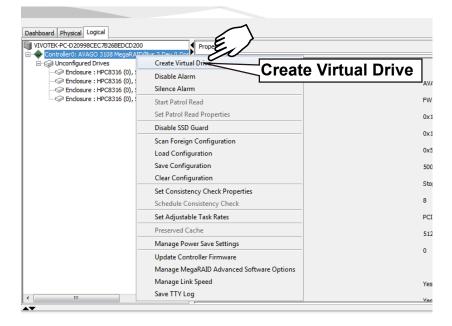
4. A Dashboard view will appear. Click the Logical tab.

🗃 MegaRAID	Storage Manager - 14.02.01	.03				
Manage Go T	o Log Tools Help					
: 🛡 🧐 🕜	2 40 🕜					
-	ysical Logical AVAGO 3108 MegaRAID (Bus 2	,Dev 0)				
Properties			Usage			Background Operations
 Status: Enclosures 	📀 Optimal : 0					Virtual drive operations in progress: 0
III Backplanes				Total capacit 9.095 TB	icity:	
Drives:	4		Confi	Configure	ed Capacity:	Drive operations in progress: 0
💓 Drive group	ps: 0				red Canacity:	
间 Virtual Driv			100%	9.095 TB	ured Capacity:	
View server	profile					More details
	vanced Software Options		Actions			Help
MegaRAID Fa		Enabled	Create virtual drive			How to use MSM?
MegaRAID RA		Enabled	Create CacheCade™ - SS	SD Caching		How to create virtual drive?
MegaRAID RA		Enabled	Load configuration			How to enable MegaRAID Advanced Softwa
Manage Meg	aRAID Advanced Software Op	tions	Update firmware			Glossary
			Silence alarm			
▲▼			1			·
ID	Error Level	Date / Time		De	escription	
10000	[Information, 0]	2016-01-09, 10:5				erver User: VIVOTEK, Client: 192.168.6.203,
44 505	[Information, 0] [Information, 0]	2016-01-09, 10:4 31 seconds from				tablished since power on: Time 2016-01-09, 10
505 [Information, 0] 31 seconds fro		par seconds from	n reboot Controller ID: 0 Controller operating temperature within r		a operating temperature within normal range, tu	

5. Left-click to select the AVAGO MegaRAID controller, and then right-click to display a command menu.



6. Click on Create Virtual Drive.



7. The **Create Virtual Drive** wizard will start. Click to select the **Advanced** mode. Then click the Next button to proceed.

Create Virtual Drive - Choose mode	×
	Avago
This wizard will help you quickly create virtual drives.	
Choose how to create the virtual drive:	
Specify in number of settings and have the system pick drives for you. This is the easier virtual of the system pick drives for you. This is the system pick drives for you. The system pick drives for you. This is the system pick drives for you. Thi	st way to create a
Choose additional settings and customize virtual drive creation. This option provides greater f virtual drives for your specific requirements.	lexibility when creating
	E
	Cancel Next Help

8. Select a **RAID level**, and then select multiple disk drives as the members of your drive group. Left-click to select a disk drive, and click **Add** to add it to group. You do not need to select the Data protection option.

	Create Drive Group - Drive Group Settings	×
	Create the drive group by specifying the RAID la	Ecurity method.
	RAID level:	
RAID 5	RAID 5	This RAID level is suitable for multi-user environments(database or file system) with large IO size and high proportion of read activity.
Select	Drive security method:	
RAID 0	Select 👻	Drive security will make the virtual drive secure by applying encryption logic to
RAID 1	Data protection:	underlying data in the drive.
RAID 5	Disable	Data Protection is a guard that detects corruption of data on media; thereby preventing
RAID 6 RAID 00 - Spanned Drive Group	Uisable	system errors caused b ata corruption (SDC).
RAID 00 - Spanned Drive Group		
	Select unconfigured drives:	Drive groups:
	Drive Type	Add >> Controller0: AVAGO 3108 MegaRAID(Bus 2,Dev
	Endosure : HPC8316 (0 SATA 149.05	Aud >> Enclosure : HPC8316 (0), Slot: 0: SATA:
	Enclosure : HPC8316 (0 SATA 1.819 TB Enclosure : HPC8316 (0 SATA 2.729 TB	Add Hot Spare >
	Contraction (0 SATA 2.729 18	<< Remove
		Create Drive Group Create Span
		Cancel Back Next Help
	-	

Refer to the next section: **RAID Basics** on page 44, for details about RAID levels.

9. Click on the Drive Group 0 entry you have just configured. The **Create Drive Group** button will become available. Click Next to proceed.

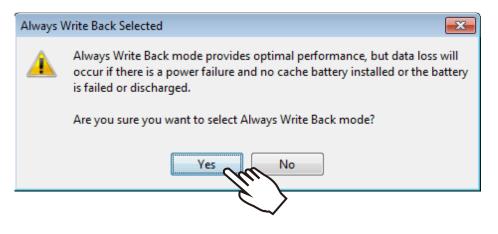
Create Drive Group - Drive Grou	p Settings	
reate the drive group by specifying t AID level: RAID 5	the RAID level and D	Drive security method.
rive security method: ielect ata protection:	000	Drive security will make the virtual dri underlying data in the drive.
Select unconfigured drives:	e Capa	Data Protection is a guard that detects corruption system errors caused by silent data corruption (SD Drive groups: Controller0: AVAGO 3108 MegaRAID(Bus 2,1
	e Capa	Add >> Image: Construction of the state of the sta
		Create Drive Group Create Space

9. Select the following key parameters: Initialization State: Fast Initialization, Strip size: 64KB, RAID policy: No Read Ahead, Write policy: Always Write Back.

These are important parameters to the disk array performance, and have to be correctly configured. Click **Create Virtual Drive**.

Create Virtual Dr	ive - Virtual drive settings		×
			Avago
Specify parameters f	or the new virtual drive.	Drive groups:	
Virtual drive name:	VD_0		3108 MegaRAID(Bus 1,Dev 0,Domain 0) AID 0: Available Capacity: 2.729 TB
Capacity:	2.729 - Units: TB -	Fast Init	ialization
Initialization state:	Fast Initialization		1
Strip size:	64 KB 👻	64 KB	
Read policy:	No Read Ahead 🗸	🥂 No Re	ead Ahead
Write policy:	Always Write Back 🔻	Alway	s Write Back
I/O policy:	Direct IO 🔻		
Access policy:	Read Write 👻		
Disk cache policy:	Disabled 🗸		
Update Virtual Dr	rive Create Virtual Drive	Remove Virtual Drive	
		Ca	ancel Back Next Help

10. Click **Yes** to leave the Write Back concern message.

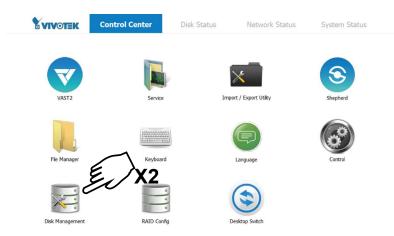


11. The wizard may prompt for another virtual drive. Multiple virtual drives can be created from a physical drive group. Repeat the process to create more 4-member Virtual Drives. When done, click to select the **Virtual Drive 0,VD_0**, and then click **Next** to proceed.

Create Virtual D	rive - Virtual drive settings	×
		Avago
Specify parameters	for the new virtual drive.	Drive groups:
Virtual drive name:	VD_0	Controller0: AVAGO 3108 MegaRAID(Bus 2 Drive Group0: RAID 5: Available Capa
Capacity:	445.594 🔪 Units: GB 👻	Intual Drive 0, VD_0:445.594 GB
Initialization state:	Fast Initialization 👻	
Strip size:	64 KB 👻	
Read policy:	No Read Ahead 👻	
Write policy:	Always Write Back 👻	
I/O policy:	Direct IO 👻	
Access policy:	Read Write 👻	
Disk cache policy:	Disabled 👻	
Update Virtual	Drive Create Virtual Drive	Remove Virtual Drive
		Cancel Back Next Help

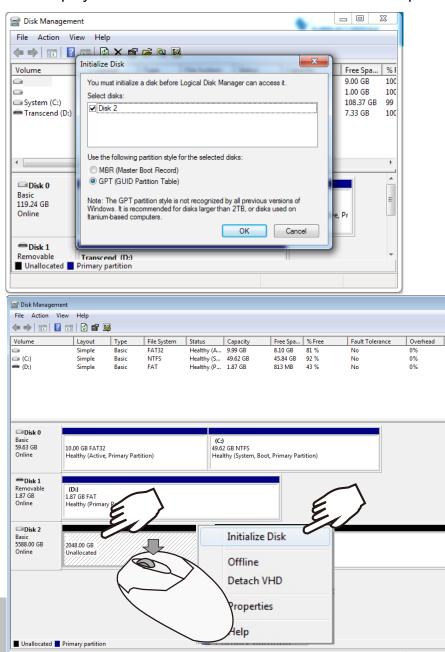
12. The Virtual Drive is instantly created. Click **OK**, and then click **Finish** to close the wizard. You can then terminate the MegaRAID utility.

Create Virtual Drive - Summary	Strength Sec	
	A	
	<u>Ava</u>	GO 🛛
	e corrections. The virtual drive(s) will be created when ye	dick finish.
Summary:		
Drive group name:	Drive Group0	
RAID Level:	RAID 5	
Number of drives used:	4	
Drive security method:	No Encryption	
Data Protection:	Disabled	
Hot Spare	No	
Total capacity:	445.594 GB	
Virtual drive 1 name:	VD 0	
Capacity:	445.594 GB	
		- Create Virtual Drive - Summary
1		Eu Ava
•		40 EVE
	Cancel Back Fini	
		Review the summary and go back if you need to make corrections. The virtual drive(s) will be created when yo
seast cotting target II as invalid		
		Summary:
		Drive group name: Drive Group0
		RAID Level: RAID 5
		Number of drives us Treate Virtual Drive - complete
		Drive security meth
		Data Bratastiant
		The virtual drive(s) successfully created
		Hot Spare
		Total capacity: OK
		Virtual drive 1 nam
		Capacity: 445.594 GB
		•
		Cancel Back Fini



13. Double-click on the **Disk Management** shortcut on the desktop to open the utility.

14. The virtual drive you created should appear as a new disk partition. You need to initialize and format the partition before using the disk capacity. Left-click to select and then right-click to display the command menu. Click **Initialize Disk** to proceed.



User's Manual - 35

15. Select **GPT** (GUID Partition Table), and then click **OK** to proceed. This window may automatically pop up when Disk Management is started.

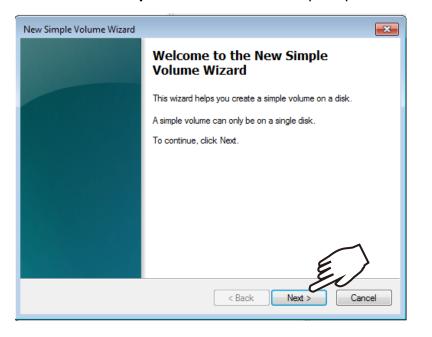
Initialize Disk	×
You must initialize a disk before Logical Disk Manager can access it.	
Select disks:	
Disk 2]
Use the ing partition style for the selected disks:	
○ Master Boot Record)	
GPT (GUID Partition Table)	
Note: The GPT partition style is not recognized by all previous versions of Windows. It is recommended for disks larger than 2TB, or disk on Itanium-based computers.	
OK Cancel	

16. Once initialized, you can create a new volume. Right-click to display the **New Simple Volume** command. Click to proceed.

Please do not format drive C:. Doing so will disable the system.

Basic 59.63 GB Online	10.00 GB FAT32 Healthy (Active, Primary Partition)	(C:) 49.62 GB NTFS Healthy (System, Boot, Primary Partition)
Disk 1 Removable 1.87 GB Online	(D:) 1.87 GB FAT Healthy (Primary Partition)	
Basic	TITITI E,	
5588.00 GB Online	2048.00 GB Unallocated	E
5588.00 GB		New Simple Volume
5588.00 GB		New Simple Volume New Spanned Volume New Striped Volume
5588.00 GB		New Spanned Volume
5588.00 GB		New Spanned Volume New Striped Volume
5588.00 GB		New Spanned Volume New Striped Volume New Mirrored Volume

17. The New Simple Volume Wizard will prompt. Click Next to proceed.



18. Leave the volume size unchanged. Click Next to proceed.

New Simple Volume Wizard	
Specify Volume Size Choose a volume size that is between t	he maximum and minimum sizes.
Maximum disk space in MB: Minimum disk space in MB: Simple volume size in MB:	5721982 8 5721982
	< Back Next > Cancel

19. When prompted to assign a drive letter, click Next to proceed.

New Simple Volume Wiz	ard	Numero, A	x
Assign Drive Letter For easier access,		etter or drive path to your partitior	1.
	ving drive letter: lowing empty NTFS folde drive letter or drive path	Browse	
		< Back Next >	Cancel

20. On the **Format Partition** page, select the **Allocation unit size** as **64KB**. When done, click Next to proceed.

	New Simple Volume Wizard
	Format Partition To store data on this partition, you must format it first.
	Choose whether you want to format this volume, and if so, what settings you want to use.
	O not format this volume
	Format this volume with the following settings:
	File system: NTFS 💌
	Allocation unit size:
	Volume label: 512
	Perform a quick format
	Enable file and folder cor 8112
64	
	< Back Next > Cancel
	<i>Im</i>

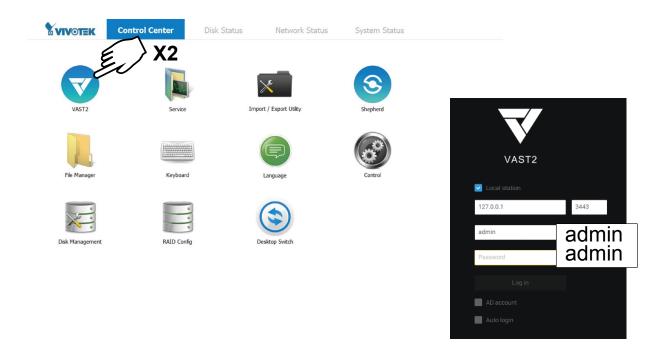
21. Click Finish to end the wizard.

New Simple Volume Wizard		×
	Completing the New Simple Volume Wizard	
	You have successfully completed the New Simple Volume Wizard.	
	You selected the following settings: Volume type: Simple Volume Disk selected: Disk 2 Volume size: 5721982 MB Drive letter or path: E: File system: NTFS Allocation unit size: Default Volume label: New Volume Ourick format: Yes To close this wizard, click Finish.	
	< Back Finish Cance	1

22. The formatting process will run in the background. When done, the new volume shall be indicated as a healthy new volume. Close the Disk Management window.

Online	Healthy (Active, Primary Partition)				
Disk 1 Removable 1.87 GB Online	(D:) 1.87 GB FAT Healthy (Primary Partition)				
Disk 2 Basic 5587.88 GB Online	5587.87 GB Formatting				
	р				
Disk 1 Removable 1.87 GB Online	(D:) 1.87 GB FAT Healthy (Primary Partition)				
Disk 2 Basic 5587.88 GB Online	New Volume (E:) 5587.87 GB NTFS Healthy (Primary Partition)				

23. Start VIVOTEK **VAST** management software by double-clicking its shortbut. Enter **admin** and **admin** as the User Name and default Password. You can change the password later in the utility. Click **Log in** to proceed.



Top row	Control Cente	r: the default desktop.					
	Disk Status: Displays the current storage volume status (system drive and RAID volumes).						
	Network Status: Displays the information for the current network connections.						
	System Statu	s: Displays the current system status, license information, and VAST service.					
Desktop Shortcuts							
	VAST2	Starts the VAST2 recording and management software.					
	Service	ce Enables you to start, stop, or restart the VAST server instance.					
	Import/Export	port Allows you to import or export VAST configurations.					
	Shepherd	Use the Shepherd utility to locate cameras within your network.					
	File Manager	Provides access to the files in system disk drive volumes.					
	Keyboard	Toggles the virtual keyboard in case you do not have a physical keyboard.					
	Language	Changes the UI language					
	Control	Opens the operating system's control panel.					
	Disk	Starts the Disk Management utility in Windows.					
	Managment						
	RAID Config.	Starts the RAID card storage configuration utility.					

24. The first time the VAST2 server is started, a configuration wizard will prompt to guide you through the basic configuration. Select drive E:/ as the default location for the server database.

Set up database
Setup a database path is required at the first time before starting Image: Drive time before starting Drive time before starting <t< td=""></t<>

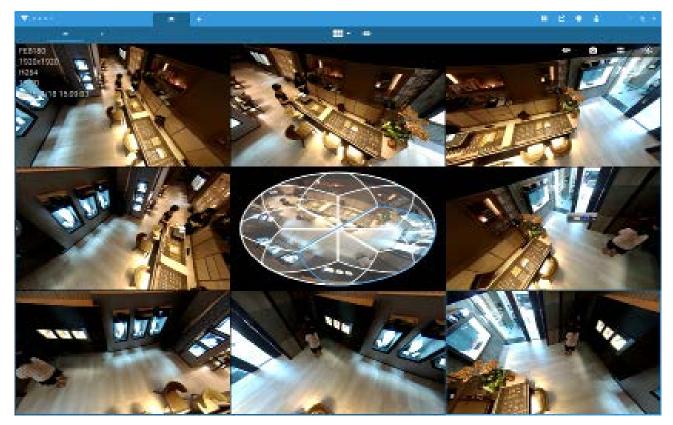
25. The next screen provides a list of all cameras in the local network. Select the cameras of your choice. Enter the credentials for making the connection with the network cameras. When done, click the **Next** button to proceed.

	Add device				- = ×	
	Add device					Authorize 1 selected devices
Add 7 devices Add device Add device	rand(onvif/vvtk) Authorize	+ 🖦				192.168.5.125 00-02-D1-3E-1D-97
SE P	▲ MAC	Port	Model	Bra		root
	9.254.5.99	80 80	XNB-6005 SND-6011R	ONVIF		•••••
V 16	9.254.43.19 9.254.209.189	80 80	A8004-VE FE9191	ONVIF		
	0.254.218.164	80	P5544 IT9389-HT	ONVIF		Apply Cancel
Ready to use	9.254.228.59 9.254.238.59	80	FD9389-HTV			
	Synchronize c	amera time with	system Next	Cancel		

26. Select the recording volumes, such as the E:/ volume you just created. When done, click the **Ready to use** button.

0.	Schedule	eve teoropistel	ng option		
Add daves	Ĩ				
Recording options	Continuous recordings	Events only	None	Customize	
Contraction Preserved To Large	Storage 🔹 👐	Ē	>		
	D:	e			Ð
	Back				Ready to use Concel

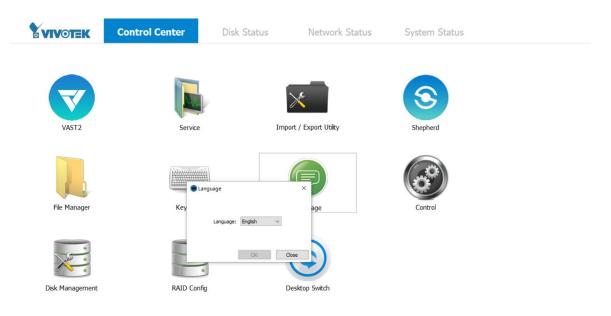
27. You should then enter the Liveview of the VAST2 software. Follow the discussions in later sections for how to configure your VAST2 deployment.





- 1. Cameras and the NVR must reside in the same subnet. Otherwise, the NVR will not be able to recruit them into a recording configuration.
- 2. It is recommended all network cameras use static IPs. If you let a DHCP server assign IPs to these cameras, IPs may be changed later and the NVR may not recognize them.

If preferred, change the language of UI text using the Language shortcut on the desktop.



0

RAID Basics

MIMPORTANT:

For a RAID volume configuration, it is recommended you use hard drives of the same model featuring the same capacity and rotation speed. It is also preferred that these drives are running the same version of firmware.

A Redundant Array of Independent Disks is an array, or group, of multiple independent physical drives that provide high performance and fault tolerance. A RAID drive group improves I/O performance and reliability. The RAID drive group appears to the host computer as a single storage volume or as multiple virtual units. An I/O transaction is expedited because several drives can be accessed simultaneously.

A RAID drive group improves data storage reliability and fault tolerance compared to single drive storage. Data loss resulting from a drive failure can be prevented by reconstructing missing data from the remaining drives. The benefits of RAID come from the improvement of I/O performance and the increased reliability.

What are the Virtual drives?

Virtual drives are drive groups that are available to the operating systems. The storage space in a virrtual drive comes from all the members in the drive group.

The RAID functions available for virtual drives include:

- Hot spare drives.
- Drive group and virtual drive configurations.
- Initializing one or more virtual drives.
- Individual access to controllers, virtual drives, and disk drives.
- Failed drive rebuild.
- Verification of redundancy data in virtual drives using RAID levels 1, 5, 6, 10, 50, and 60.
- Reconstructing virtual drives after the RAID levels or adding a drive to a drive group.
- Indepently selecting a host controller to work for.

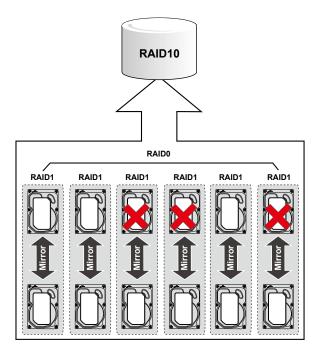
RAID configuration components

- Drive group: a group of physical drives. These drives will be managed in partitions known as virtual drives.
- Virtual drive: a partition in a drive group made of continguous data segments from the individual disk drives. A virtual drive can consist of the following components:
 - An entire drive group.
 - More than one entire drive group.
 - A part of drive group.
 - Parts of more than one drive group.
 - A combination of any two of the conditions above.

RAID Fault Tolerance

RAID Level	Number of Tolerable Drive Failures
0	No fault tolerance
1	1, each drive group
5	1
6	2
10	multiple, as long as each failure is in a separate drive group
50	1 in each drive group
60	2 in each drive group

For example, if disk failure occurs in different drive groups, a RAID10 configuration can tolerate multiple drive failures. In each RAID1 drive group, data is mirrored to a counterpart disk drive. Data remains intact if one disk drive should fail in each drive group.



Consistency Check

The consistency check operation verifies the correctness of the data in virtual drives that use RAID levels 1, 5, 6, 10, 50, and 60. RAID0 does not provide data redundancy. In a system with parity, check consistency means calculating the data on one drive and comparing the results to the contents of the parity drive.

Background Initialization

Background initialization is a check for media errors on the drives when you create a virtual drive. It is an automatic operation that starts five minutes after you create a virtual drive. This check ensures that striped data segments are the same on all of the drives in the drive group.

Background initialization is similar to a consistency check. The difference between the two is that a background initialization is forced on new virtual drives and a consistency check is not.

New RAID 5 virtual drives and new RAID 6 virtual drives require a minimum number of drives for a background initialization to start. If fewer drives exist, the background initialization does not start. The background initialization needs to be started manually. The following number of drives are required:

New RAID 5 virtual drives must have at least five drives for background initialization to start.

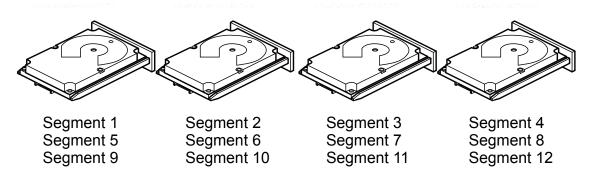
New RAID 6 virtual drives must have at least seven drives for background initialization to start.

The default and recommended background initialization rate is 30 percent. Before you change the rebuild rate, you must stop the background initialization or the rate change will not affect the background initialization rate. After you stop background initialization and change the rebuild rate, the rate change takes effect when you restart background initialization.2.1.7Patrol Read

Disk Striping

Disk striping lets you write data across multiple drives instead of just one drive. Disk striping involves partitioning each drive storage space into stripes that can vary in size from a minimum of 64 KB to 1 MB for MegaRAID controllers and 64 KB for Integrated MegaRAID controllers. The LSISAS2108 controller allows stripe size from 8 KB to 1 MB. These stripes are interleaved in a repeated sequential manner. The combined storage space is composed of stripes from each drive. It is recommended that you keep stripe sizes the same across RAID drive groups.

For example, in a four-disk system using only disk striping (used in RAID level 0), segment 1 is written to disk 1, segment 2 is written to disk 2, and so on. Disk striping enhances performance because multiple drives are accessed simultaneously, but disk striping does not provide data redundancy.



Stripe Width

Stripe width is the number of drives involved in a drive group where striping is implemented. For example, a four-disk drive group with disk striping has a stripe width of four.

Stripe Size

The stripe size is the length of the interleaved data segments that the RAID controller writes across multiple drives, not including parity drives. For example, consider a stripe that contains 1 MB of drive space and has 64 KB of data residing on each drive in the stripe. In this case, the stripe size is 1 MB and the strip size is 64 KB.

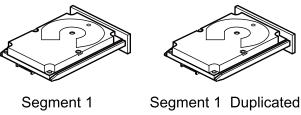
Strip Size

The strip size is the portion of a stripe that resides on a single drive.

Disk Mirroring

With disk mirroring (used in RAID 1 and RAID 10), data written to one drive is simultaneously written to another drive. The primary advantage of disk mirroring is that it provides 100 percent data redundancy. Because the contents of the disk are completely written to a second disk, data is not lost if one disk fails. In addition, both drives contain the same data at all times, so either disk can act as the operational disk. If one disk fails, the contents of the other disk can run the system and reconstruct the failed disk.

Disk mirroring provides 100 percent redundancy, but it is expensive because each drive in the system must be duplicated. The following figure shows an example of disk mirroring.



Segment 2 Segment 3 Segment 4



Segment 2 Duplicated Segment 3 Duplicated Segment 4 Duplicated

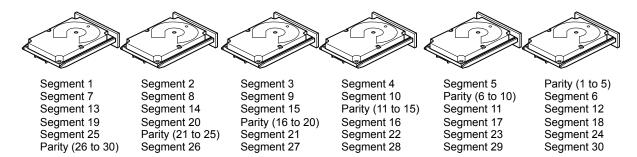
3 01080-00

Parity

Parity generates a set of redundancy data from two or more parent data sets. The redundancy data can be used to reconstruct one of the parent data sets in the event of a drive failure. Parity data does not fully duplicate the parent data sets, but parity generation can slow the write process. In a RAID drive group, this method is applied to entire drives or stripes across all of the drives in a drive group. The types of parity are described in the following table.

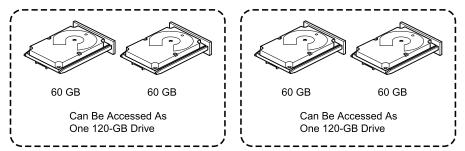
Parity Type	Description
Dedicated	The parity data on two or more drives is stored on an additional disk.
Distributed	The parity data is distributed across more than one drive in the system.

A RAID 5 drive group combines distributed parity with disk striping. If a single drive fails, it can be rebuilt from the parity and the data on the remaining drives. An example of a RAID 5 drive group is shown in the following figure. A RAID 5 drive group uses parity to provide redundancy for one drive failure without duplicating the contents of entire drives. A RAID 6 drive group also uses distributed parity and disk striping, but adds a second set of parity data so that it can survive up to two drive failures.



Disk Spanning

Disk spanning allows multiple drives to function like one big drive. Spanning overcomes lack of disk space and simplifies storage management by combining existing resources or adding relatively inexpensive resources. For example, four 20-GB drives can be combined to appear to the operating system as a single 80-GB drive. Spanning alone does not provide reliability or performance enhancements. Spanned virtual drives must have the same stripe size and must be contiguous. In the following figure, RAID 1 drive groups are turned into a RAID 10 drive group.



Spanning two contiguous RAID 0 virtual drives does not produce a new RAID level or add fault tolerance. It does increase the capacity of the virtual drive and improves performance by doubling the number of spindles.

Spanning for RAID 00, RAID 10, RAID 50, and RAID 60 Drive Groups

The following table describes how to configure RAID 00, RAID 10, RAID 50, and RAID 60 drive groups by spanning. The virtual drives must have the same stripe size and the maximum number of spans is 8. The full drive capacity is used when you span virtual drives; you cannot specify a smaller drive capacity.

Level	Description
00	Configure a RAID 00 by spanning two or more contiguous RAID 0 virtual drives, up to the
	maximum number of supported devices for the controller.
10	Configure RAID 10 by spanning two or more contiguous RAID 1 virtual drives, up to
	the maximum number of supported devices for the controller. A RAID 10 drive group
	supports a maximum of 8 spans. You must use an even number of drives in each RAID
	virtual drive in the span. The RAID 1 virtual drives must have the same stripe size.
50	Configure a RAID 50 drive group by spanning two or more contiguous RAID 5 virtual
	drives. The RAID 5 virtual drives must have the same stripe size.
60	Configure a RAID 60 drive group by spanning two or more contiguous RAID 6 virtual
	drives. The RAID 6 virtual drives must have the same stripe size.

Hot Spares

A hot spare is an extra, unused drive that is part of the disk subsystem. It is usually in Standby mode, ready for service if a drive fails. Hot spares let you replace failed drives without system shutdown or user intervention. The MegaRAID SAS RAID controllers can implement automatic and transparent rebuilds of failed drives using hot spare drives, which provide a high degree of fault tolerance and zero downtime.

The RAID management software lets you specify drives as hot spares. When a hot spare is needed, the RAID controller assigns the hot spare that has a capacity closest to and at least as great as that of the failed drive to take the place of the failed drive. The failed drive is removed from the virtual drive and marked ready awaiting removal after the rebuild to a hot spare begins. You can make hot spares of the drives that are not in a RAID virtual drive.

You can use the RAID management software to designate the hot spare to have enclosure affinity, which means that if drive failures are present on a split backplane configuration, the hot spare will be used first on the backplane side in which it resides. If the hot spare is designated as having enclosure affinity, it tries to rebuild any failed drives on the backplane in which it resides before rebuilding any other drives on other backplanes.

The hot spare can be of two types:

- Global hot spare
- Dedicated hot spare

Global Hot Spare

Use a global hot spare drive to replace any failed drive in a redundant drive group as long as its capacity is equal to or larger than the coerced capacity of the failed drive. A global hot spare defined on any channel should be available to replace a failed drive on both channels.

Dedicated Hot Spare

Use a dedicated hot spare to replace a failed drive only in a selected drive group. One or more drives can be designated as a member of a spare drive pool. The most suitable drive from the pool is selected for failover. A dedicated hot spare is used before one from the global hot spare pool.

Hot spare drives can be located on any RAID channel. Standby hot spares (not being used in RAID drive group) are polled every 60 seconds at a minimum, and their status made available in the drive group management software. RAID controllers offer the ability to rebuild with a disk that is in a system but not initially set to be a hot spare.

Observe the following parameters when using hot spares:

- Hot spares are used only in drive groups with redundancy: RAID levels 1, 5, 6, 10, 50, and 60.
- A hot spare connected to a specific RAID controller can be used to rebuild a drive that is connected only to the same controller.
- You must assign the hot spare to one or more drives through the controller BIOS or use drive group management software to place it in the hot spare pool.
- A hot spare must have free space equal to or greater than the drive it replaces. For example, to replace a 500-GB drive, the hot spare must be 500-GB or larger.

Disk Rebuilds

When a drive in a RAID drive group fails, you can rebuild the drive by re-creating the data that was stored on the drive before it failed. The RAID controller re-creates the data using the data stored on the other drives in the drive group. Rebuilding can be performed only in drive groups with data redundancy, which includes RAID 1, 5, 6, 10, 50, and 60 drive groups.

The RAID controller uses hot spares to rebuild failed drives automatically and transparently, at user-defined rebuild rates. If a hot spare is available, the Rebuild operation can start automatically when a drive fails. If a hot spare is not available, the failed drive must be replaced with a new drive so that the data on the failed drive can be rebuilt.

The failed drive is removed from the virtual drive and marked ready awaiting removal when the Rebuild operation to a hot spare begins. If the system goes down during a Rebuild operation, the RAID controller automatically resumes the rebuild after the system reboots.

When the Rebuild operation to a hot spare begins, the failed drive is often removed from the virtual drive before management applications detect the failed drive. When this removal occurs, the event logs show the drive rebuilding to the hot spare without showing the failed drive. The formerly failed drive will be marked as ready after a Rebuild operation begins to a hot spare. If a source drive fails during a rebuild to a hot spare, the Rebuild operation fails, and the failed source drive is marked as offline. In addition, the rebuilding hot spare drive is changed back to a hot spare. After a Rebuild operation fails because of a source drive failure, the dedicated hot spare is still dedicated and assigned to the correct drive group, and the global hot spare is still global.

An automatic drive Rebuild operation will not start if you replace a drive during a RAID-level migration. The Rebuild operation must be started manually after the expansion or migration procedure is complete. (RAID-level migration changes a virtual drive from one RAID level to another.)

Hot Swap

A hot swap is the manual replacement of a defective drive unit while the computer is still running. When a new drive has been installed, a Rebuild operation occurs automatically if these situation occurs:

- The newly inserted drive is the same capacity as or larger than the failed drive.
- The newly inserted drive is placed in the same drive bay as the failed drive it is replacing.

The RAID controller can be configured to detect the new drives and rebuild the contents of the drive automatically.

Drive States

A drive state is a property indicating the status of the drive. The drive states are described in the following table.

Parity Type	Description	
Online	A drive that can be accessed by the RAID controller and is part of the virtual drive.	
Unconfigured Good	A drive that is functioning normally but is not configured as a part of a virtual drive or as a	
	hot spare.	
Hot Spare	A drive that is powered up and ready for use as a spare in case an online drive fails.	
Failed	A drive that was originally configured as Online or Hot Spare, but on which the firmware	
	detects an unrecoverable error.	
Rebuild	A drive to which data is being written to restore full redundancy for a virtual drive.	
Unconfigured Bad	A drive on which the firmware detects an unrecoverable error; the drive was Unconfigured	
	Good or the drive could not be initialized.	
Missing	A drive that was Online but which has been removed from its location.	
Offline	A drive that is part of a virtual drive but which has invalid data as far as the RAID	
	configuration is concerned.	
Shield State	An interim state of physical drive for diagnostic operations.	
Copyback	A drive that has replaced the failed drive in the RAID configuration.	

Virtual Drive States

Parity Type	Description	
Online	The virtual drive operating condition is good. All configured drives are online.	
Degraded	The virtual drive operating condition is not optimal. One of the configured drives has	
	failed or is offline.	
Partial Degraded	The operating condition in a RAID 6 virtual drive is not optimal. One of the configured	
	drives has failed or is offline. A RAID 6 drive group can tolerate up to two drive failures.	
Failed	The virtual drive has failed.	
Offline	The virtual drive is not available to the RAID controller.	

The virtual drive states are described in the following table.

Beep Codes

An alarm sounds on the MegaRAID controller when a virtual drive changes from an optimal state to another state, when a hot spare rebuilds, and for test purposes.

Parity Type	Virtual Drive State	Beep Code
RAID 0 virtual drive loses a virtual drive	Offline	3 seconds on and 1 second off
RAID 1 virtual drive loses a mirror drive	Degraded	1 second on and 1 second off
RAID 1 virtual drive loses both drives	Offline	3 seconds on and 1 second off
RAID 5 virtual drive loses one drive	Degraded	1 second on and 1 second off
RAID 5 virtual drive loses two or more	Offline	3 seconds on and 1 second off
drives		
RAID 6 virtual drive loses one drive	Partially degraded	1 second on and 1 second off
RAID 6 virtual drive loses two drives	Degraded	1 second on and 1 second off
RAID 6 virtual drive loses more than two	Offline	3 seconds on and 1 second off
drives		
A hot spare completes the Rebuild	B/A	1 second on and 3 seconds off
process and is brought into a drive group		
A copy back occurs after a Rebuild	Optimal	1 second on and 3 seconds off
operation completes		

RAID Levels

The RAID controller supports RAID levels 0, 00, 1, 5, 6, 10, 50, and 60. The supported RAID levels are summarized in the following section.

In addition, the RAID controller supports independent drives (configured as RAID 0 and RAID 00 drive groups) The following sections describe the RAID levels in detail.

Summary of RAID Levels

A RAID 0 drive group uses striping to provide high data throughput, especially for large files in an environment that does not require fault tolerance.

A RAID 1 drive group uses mirroring so that data written to one drive is simultaneously written to another drive. The RAID 1 drive group is good for small databases or other applications that require small capacity but complete data redundancy.

A RAID 5 drive group uses disk striping and parity data across all drives (distributed parity) to provide high data throughput, especially for small random access. A RAID 6 drive group uses distributed parity, with two independent parity blocks per stripe, and disk striping.

A RAID 6 virtual drive can survive the loss of any two drives without losing data. A RAID 6 drive group, which requires a minimum of three drives, is similar to a RAID 5 drive group. Blocks of data and parity information are written across all drives. The parity information is used to recover the data if one or two drives fail in the drive group.

A RAID 00 drive group is a spanned drive group that creates a striped set from a series of RAID 0 drive groups. A RAID 10 drive group, a combination of RAID 0 and RAID 1 drive groups, consists of striped data across mirrored spans.

A RAID 10 drive group is a spanned drive group that creates a striped set from a series of mirrored drives. A RAID 10 drive group allows a maximum of 8 spans. You must use an even number of drives in each RAID virtual drive in the span. The RAID 1 virtual drives must have the same stripe size. A RAID 10 drive group provides high data throughput and complete data redundancy but uses a larger number of spans.

A RAID 50 drive group, a combination of RAID 0 and RAID 5 drive groups, uses distributed parity and disk striping. A RAID 50 drive group is a spanned drive group in which data is striped across multiple RAID 5 drive groups. A RAID 50 drive group works best with data that requires high reliability, high request rates, high data transfers, and medium-to-large capacity.

Having virtual drives of different RAID levels, such as RAID Level0 and RAID Level5, in the same drive group is not allowed. For example, if an existing RAID5 virtual drive is created out of partial space in an array, the next virtual drive in the array has to be RAID Level 5 only.

A RAID 60 drive group, a combination of RAID level 0 and RAID Level 6, uses distributed parity, with two independent parity blocks per stripe in each RAID set, and disk striping. A RAID 60 virtual drive can survive the loss of two drives in each of the RAID 6 sets without losing data. A RAID 60 drive group works best with data that requires high reliability, high request rates, high data transfers, and medium-to-large capacity.

The MegaSR controller supports the standard RAID levels – RAID0, RAID1, RAID5, and RAID10. The MegaSR controller comes in two variants, SCU and AHCI, both supporting a maximum of eight physical drives. A maximum of eight virtual drives can be created (using RAID0, RAID 1, RAID5, and RAID10 only) and controlled by the MegaSR controller. One virtual drive can be created on an array (a maximum of eight if no other virtual drives are already created on the MegaSR controller), or you can create eight arrays with one virtual drive each. However, on a RAID10 drive group, you can create only one virtual drive on a particular array.

RAID 0 Drive Groups

A RAID 0 drive group provides disk striping across all drives in the RAID drive group. A RAID0 drive group does not provide any data redundancy, but the RAID 0 drive group offers the best performance of any RAID level. The RAID 0 drive group breaks up data into smaller segments, and then stripes the data segments across each drive in the drive group. The size of each data segment is determined by the stripe size. A RAID 0 drive group offers high bandwidth.

By breaking up a large file into smaller segments, the RAID controller can use both SAS drives and SATA drives to read or write the file faster. A RAID 0 drive group involves no parity calculations to complicate the write operation. This situation makes the RAID 0 drive group ideal for applications that require high bandwidth but do not require fault tolerance. The following table provides an overview of the RAID 0 drive group. The following figure provides a graphic example of a RAID 0 drive group.

RAID level 0 is not fault tolerant. If a drive in a RAID 0 drive group fails, the entire virtual drive (all drives associated with the virtual drive) fails.

Uses	Provides high data throughput, especially for large files. Any environment that does not	
	require fault tolerance.	
Strong points	Provides increased data throughput for large files.	
	No capacity loss penalty for parity.	
Weak points	Does not provide fault tolerance or high bandwidth.All data is lost if any drive fails.	
Drives	1 to 32	



Segment 1 Segment 3 Segment 5 Segment 7

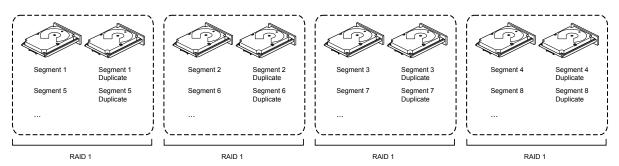


Segment 2 Segment 4 Segment 6 Segment 8

RAID 1 Drive Groups

In RAID 1 drive groups, the RAID controller duplicates all data from one drive to a second drive in the drive group. A RAID 1 drive group supports an even number of drives from 2 through 32 in a single span. The RAID1 drive group provides complete data redundancy, but at the cost of doubling the required data storage capacity. The following table provides an overview of a RAID1 drive group. The following figure provides a graphic example of a RAID1 drive group.

Uses	Use RAID 1 drive groups for small databases or any other environment that requires fault	
	tolerance but small capacity.	
Strong points	Provides complete data redundancy. A RAID 1 drive group is ideal for any application that requires fault tolerance and minimal capacity.	
Weak points	Requires twice as many drives. Performance is impaired during drive rebuilds.	
Drives	2 through 32 (must be an even number of drives)	



RAID 5 Drive Groups

A RAID 5 drive group includes disk striping at the block level and parity. Parity is the data's property of being odd or even, and parity checking is used to detect errors in the data. In RAID5 drive groups, the parity information is written to all drives. A RAID5 drive group is best suited for networks that perform a lot of small input/output (I/O) transactions simultaneously. The following table provides an overview of a RAID5 drive group. The following figure provides a graphic example of a RAID5 drive group.

Uses	Provides high data throughput, especially for large files.
	Use RAID 5 drive groups for transaction processing applications because each drive can read and write independently.
	If a drive fails, the RAID controller uses the parity drive to re-create all missing
	information. Use also for online customer service that requires fault tolerance. Use for any application that has high read request rates but random write request rates.
Strong points	Provides data redundancy, high read rates, and good performance in most environments. Provides redundancy with lowest loss of capacity.
Weak points	Not well suited to tasks requiring lots of small writes or small block write operations. Suffers more impact if no cache is used.
	Drive performance is reduced if a drive is being rebuilt.
	Environments with few processes do not perform as well because the RAID drive group overhead is not offset by the performance gains in handling simultaneous processes.
Drives	3 through 32

Segment 15

Segment 21

Segment 27

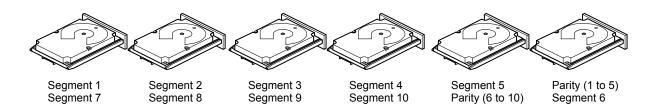
Parity (16 to 20)

Segment 14

Segment 20

Seament 26

Parity (21 to 25)



Parity (11 to 15)

Segment 16

Segment 22

Segment 28

Segment 11

Segment 17

Segment 23

Segment 29

Segment 12

Segment 18

Segment 24

Segment 30

RAID 6 Drive Groups

Segment 13

Segment 19

Segment 25

Parity (26 to 30)

A RAID6 drive group is similar to a RAID5 drive group (disk striping and parity), except that instead of one parity block per stripe, there are two. With two independent parity blocks, A RAID6 drive group can survive the loss of any two drives in a virtual drive without losing data. A RAID6 drive group provides a high level of data protection through the use of a second parity block in each stripe. Use a RAID6 drive group for data that requires a very high level of protection from loss.

In the case of a failure of one drive or two drives in a virtual drive, the RAID controller uses the parity blocks to re-create all of the missing information. If two drives in a RAID6 virtual drive fail, two drive rebuilds are required, one for each drive. These rebuilds do not occur at the same time. The controller rebuilds one failed drive, and then the other failed drive. The following table provides an overview of a RAID6 drive group.

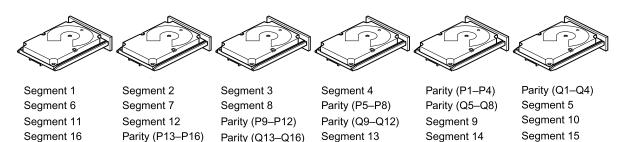
Uses	Use for any application that has high read request rates but low random or small block
	write rates.
Strong points	Provides data redundancy, high read rates, and good performance in most environments. Can survive the loss of two drives or the loss of a drive while another drive is being rebuilt.Provides the highest level of protection against drive failures of all of the RAID levels.Performance is similar to that of a RAID5 drive group.
Weak points	Not well-suited to tasks requiring a lot of small and/or random write operations.A RAID 6 virtual drive must generate two sets of parity data for each write operation, which results in a significant decrease in performance during write operations.
	Drive performance is reduced during a drive Rebuild operation.Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes.
	A RAID6 drive group costs more because of the extra capacity required by using two parity blocks per stripe.
Drives	3 through 32

The following figure shows a RAID6 drive group data layout. The second set of parity drives is denoted by Q. The P drives follow the RAID5 drive group parity scheme.

Segment 18

Segment 19

Segment 20



Segment 17

Note: Parity is distributed across all drives in the drive group.

Parity (Q17-Q20)

Parity (P17-P20)

RAID 00 Drive Groups

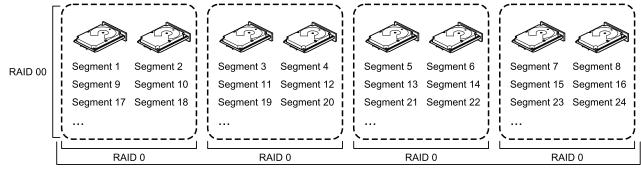
A RAID 00 drive group is a spanned drive group that creates a striped set from a series of RAID0 drive groups. A RAID00 drive group does not provide any data redundancy, but, along with the RAID0 drive group, does offer the best performance of any RAID level. A RAID00 drive group breaks up data into smaller segments and then stripes the data segments across each drive in the drive groups. The size of each data segment is determined by the stripe size. A RAID00 drive group offers high bandwidth.



RAID level 00 is not fault tolerant. If a drive in a RAID 0 drive group fails, the entire virtual drive (all drives associated with the virtual drive) fails.

By breaking up a large file into smaller segments, the controller can use both SAS drives and SATA drives to read or write the file faster. A RAID00 drive group involves no parity calculations to complicate the write operation. This situation makes the RAID00 drive group ideal for applications that require high bandwidth but do not require fault tolerance. The following table provides an overview of the RAID00 drive group. The following figure provides a graphic example of a RAID 00 drive group.

Uses	Provides high data throughput, especially for large files. Any environment that does not	
	require fault tolerance.	
Strong points	Provides increased data throughput for large files.	
	No capacity loss penalty for parity.	
Weak points	Does not provide fault tolerance or high bandwidth.	
	All data lost if any drive fails.	
Drives	2 through 256	



RAID 10

A RAID10 drive group is a combination of RAID level 0 and RAID level 1, and it consists of stripes across mirrored drives. A RAID10 drive group breaks up data into smaller blocks and then mirrors the blocks of data to each RAID1 drive group. The first RAID1 drive in each drive group then duplicates its data to the second drive. The size of each block is determined by the stripe size parameter, which is set during the creation of the RAID set. The RAID 1 virtual drives must have the same stripe size.

Spanning is used because one virtual drive is defined across more than one drive group. Virtual drives defined across multiple RAIDlevel 1 drive groups are referred to as RAID level 10, (1+0). Data is striped across drive groups to increase performance by enabling access to multiple drive groups simultaneously.

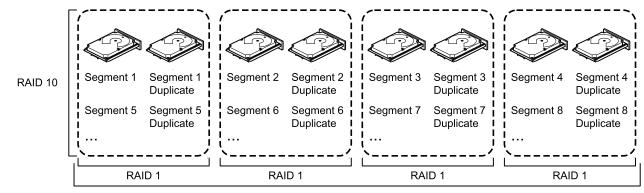
Each spanned RAID 10 virtual drive can tolerate multiple drive failures, as long as each failure is in a separate drive group. If drive failures occur, less than total drive capacity is available. Configure RAID 10 drive groups by spanning two contiguous RAID1 virtual drives, up to the maximum number of supported devices for the controller. A RAID10 drive group supports a maximum of 8spans, with a maximum of 32drives per span. You must use an even number of drives in each RAID10 virtual drive in the span.

Other factors, such as the type of controller, can restrict the number of drives supported by RAID 10 virtual drives.

Uses	Appropriate when used with data storage that needs 100 percent redundancy of mirrored drive groups and that also needs the enhanced I/O performance of RAID 0 (striped drive groups.)
	A RAID10 drive group works well for medium-sized databases or any environment that requires a higher degree of fault tolerance and moderate-to-medium capacity.
Ctrong points	
Strong points	Provides both high data transfer rates and complete data redundancy.
Weak points	Requires twice as many drives as all other RAID levels except in RAID 1 drive groups.
Drives	4 to 32 in multiples of 4 — The maximum number of drives supported by the controller
	(using an even number of drives in each RAID 10 virtual drive in the span).

The following table provides an overview of a RAID10 drive group.

In the following figure, virtual drive 0 is created by distributing data across four drive groups (drive groups 0 through3).



RAID 50

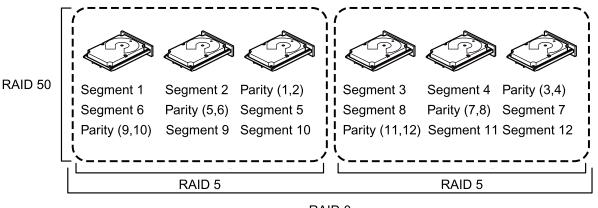
A RAID50 drive group provides the features of both RAID0 and RAID5 drive groups. A RAID50 drive group includes both distributed parity and drive striping across multiple drive groups. A RAID50 drive group is best implemented on two RAID5 drive groups with data striped across both drive groups.

A RAID50 drive group breaks up data into smaller blocks and then stripes the blocks of data to each RAID5 disk set. A RAID5 drive group breaks up data into smaller blocks, calculates parity by performing an exclusive OR operation on the blocks, and then performs write operations to the blocks of data and parity to each drive in the drive group. The size of each block is determined by the stripe size parameter, which is set during the creation of the RAID set.

A RAID level 50 drive group can support up to eight spans and tolerate up to eight drive failures, though less than total drive capacity is available. Though multiple drive failures can be tolerated, only one drive failure can be tolerated in each RAID 5 level drive group.

The following table provides an overview of a RAID50 drive group.

Uses	Appropriate when used with data that requires high reliability, high request rates, high	
	data transfer, and medium-to-large capacity.	
	Also used when a virtual drive of greater than 32 drives is needed.	
Strong points	Provides high data throughput, data redundancy, and very good performance.	
Weak points	Requires two times to eight times as many parity drives as a RAID 5 drive group.	
Drives	Eight spans of RAID 5 drive groups that contain 3 to 32 drives each (limited by the	
	maximum number of devices supported by the controller)	



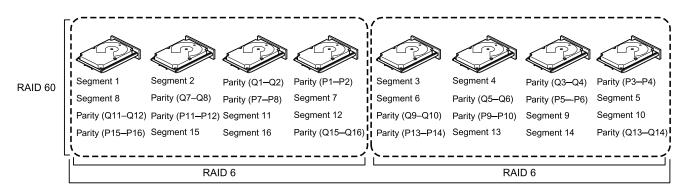
RAID 60

A RAID 60 drive group provides the features of both RAID 0 and RAID 6 drive groups, and includes both parity and disk striping across multiple drive groups. A RAID6 drive group supports two independent parity blocks per stripe. A RAID 60 virtual drive can survive the loss of two drives in each of the RAID6 drive group sets without losing data. A RAID60 drive group is best implemented on two RAID6 drive groups with data striped across both drive groups.

A RAID60 drive group breaks up data into smaller blocks and then stripes the blocks of data to each RAID6 disk set. A RAID6 drive group breaks up data into smaller blocks, calculates parity by performing an exclusive-OR operation on the blocks, and then performs write operations to the blocks of data and writes the parity to each drive in the drive group. The size of each block is determined by the stripe size parameter, which is set during the creation of the RAID set.

A RAID60 drive group can support up to 8spans and tolerate up to 16 drive failures, though less than total drive capacity is available. Two drive failures can be tolerated in each RAID 6 level drive group.

Uses	Provides a high level of data protection through the use of a second parity block in each stripe. Use a RAID60 drive group for data that requires a very high level of protection from loss.
	In the case of a failure of one drive or two drives in a RAID set in a virtual drive, the RAID controller uses the parity blocks to re-create all of the missing information. If two drives in a RAID 6 set in a RAID60 virtual drive fail, two drive Rebuild operations are required, one for each drive. These Rebuild operations can occur at the same time.
	Use for online customer service that requires fault tolerance. Use for any application that has high read request rates but low write request rates. Also used when a virtual drive of greater than 32 drives is needed.
Strong points	Provides data redundancy, high read rates, and good performance in most environments. Each RAID6 set can survive the loss of two drives or the loss of a drive while another drive is being rebuilt.Provides the highest level of protection against drive failures of all of the RAID levels.
Weak points	Not well-suited for small block write or random write operations. A RAID 60 virtual drive must generate two sets of parity data for each write operation, which results in a significant decrease in performance during write operations. Drive performance is reduced during a drive Rebuild operation. Environments with few processes do not perform as well because the RAID overhead is not offset by the performance gains in handling simultaneous processes.
	A RAID6 drive group costs more because of the extra capacity required by using two parity blocks per stripe.
Drives	A minimum of 6.



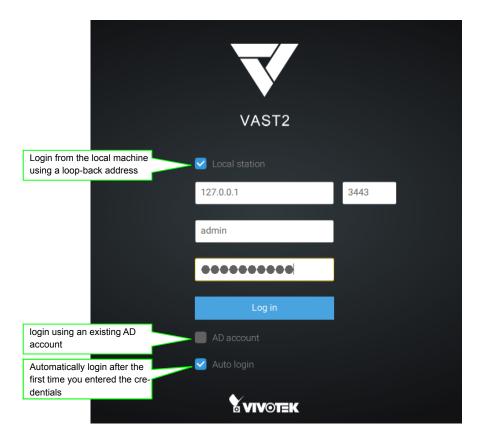
Note: Parity is distributed across all drives in the drive group.

Chapter Two VAST2 Software Configuration and Management

Log in

To log in,

- 1. Enter the server's IP address and TCP port number (3443 as the default). If logging in from the server itself, you can select the Local station checkbox.
- 2. Enter the credentials for login. The credentials were created during the installation.
- 3. You can use an existing AD ccount for login. See page 247 for user management and AD account configuration.
- 4. Auto login: After you enter the credentials for the first time, the server will not prompt for credentials the next time you start the VAST software.



Introducing VAST2

VIVOTEK VAST2 is the professional video / central management software designed for managing all VIVOTEK IP surveillance products with intuitive functions and numerous features. It supports hundreds of cameras and stations in a hierarchical structure of system for monitoring, recording, playback and event trigger management with ease-of-use and efficient control.

VAST2 integrates VIVOTEK network cameras to provide diverse solutions and applications, with the cameras for uninterrupted video recording, Smart Search II, Smart VCA, and Cybersecurity management solution. VAST2 performs remote management with full range of the server & client structure and constitutes a robust system for various applications, such as stores, banking and the public space.

New Features

- Smart Search II
- Event Search: General, Smart VCA, and Trend Micro IoT Security events.
- Alarm management with Smart VCA, Trend Micro IoT Security and new general events.
- · Alarm list enhancement: Thumbnail view, Status, and Comment.
- Manually export alarm clips.
- Automatically locks video clips when triggered by alarms.
- Sends HTTP requests to all selected cameras, incuding those under sub-stations, via one alarm configuration.
- Manually refresh selected devices to obtain the latest VADP configuration settings.
- View cells with embedded E-maps.
- Standalone player improvements for displaying VCA rules/metadata, VIVOTEK MP4/3GP, and drag and play feature.

Key Features

- Multiple monitors support on tabbed windows, configurable as live view, tour, E-map, dashboard, or alarm views.
- Supports Windows Active Directory.
- Automatic Problem Feedback mechanism.
- Add-on solutions: Failover (VAST server redundancy), Transportation, Transaction, and Data Magnet.
- Auto Streaming Size for Clients, saving decode and streaming bandwidth.
- Multiple Fisheye Dewarp modes.
- Customizable Layouts for unique camera types, e.g., corridor or panoramic.

- Supports various view settings: time, bandwidth, codec, VCA rules, etc.
- Bookmarks on the occurrence of video events with Evidence Lock.
- Customized layouts, e.g., a dewarped fisheye view, can also be displayed on standalone player.
- Log / Alarm Search & Export
- System overview Dashboard.
- VAST client on MAC machines.
- New Matrix for Video Wall Solution.
- Counting Solution with the display of VCA/Counting reports from cameras.
- Device Packs for instant support for new cameras.
- Panoramic PTZ Support.
- Cybersecurity support.

* The number of linked devices will depend on the number of licenses you purchased.

* The ability to extend devices is also subject to the network bandwidth and computer performance.

Charged Add-on Features

The following are the charged add-on features. These features will not be available unless you purchase and enable their individual licenses:

Transportation License:

- Users have the need to show their mobile server on the Google map.
- Users can use generic GPS device or VIVOTEK's mobile NVR (w/ a built-in GPS)
- We only support IP-based generic GPS.

POS Implementation:

- We provide the following for POS integration:
 - Live view with transaction data.
 - Playback with transaction data.
 - Search using keyword.
 - Highlights specific product item name.

Failover License (substations):

- We support M x N structure.
- The CMS station will be the main station for controlling and monitoring all of the active and redundant servers.
- The Failover license (substations) needs to be imported on the CMS server.

Failover License (CMS):

- We support 1 x 1 redundancy for the CMS station.
- The failover license (CMS) needs to be imported on a CMS server.

Data Magnet License:

- Data Magnet is used for integration with 3rd party data source. For example, POS data, access control, ATM data, LPR data, etc.
- We provide the following for Data Magnet integration:
 - Map the data to specific cameras.
 - Searching 3rd party data using keywords.
 - Show data with live view.
 - Set up alarms using 3rd party data.
 - Highlight specific keyword or value.

Advanced Feature License:

- Advanced License list:
 - Transportation package: Google map / GPS.
 - POS terminal.
 - Failover (Substations)
 - Failover (CMS)
 - TCP message
 - Data Magnet license.

NOTE:

1. Failover license cannot be used on hardware dongle.

2. The related configuration pages/menus will still be available even the license has not been activated.

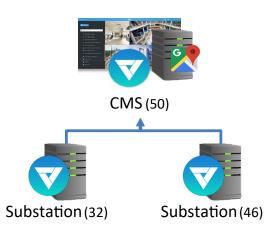
Calculation - Transportation Package: Google map + GPS



Single Server (50)

Total no. of cameras: 50 Needs 50 packages.

NOTE: camera normal usage licenses are included.



Total no. of cameras: 50 + 32 + 46 = 128 Needs 128 packages.

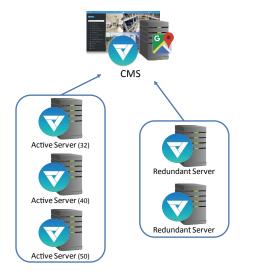
NOTE: camera normal usage licenses are included.

Calculation - POS License



Total no. of POS terminals: 2 Total no. of cameras: 50 Needs 2 POS licenses and 18 [50 - 32(free)] camera licenses.

NOTE: 32 camera channels are for free.



Calculation - Failover License

Rule:

No. of channels on the active server hosting the largest no. of cameras x the no. of redundant servers.

Channels on each active server: 32, 40, 50 No. of redundant servers: 2 Total no. of cameras: 122 (32 + 40 + 50) Needs 100 Failover licenses (50 x 2), and 90 normal camera licenses (122 - 32).

NOTE: 32 camera channels are for free. These licenses do not come with hardware dongle.

Calculation - TCP Message License



Single Server (32)



- 10 TCP messages20 camera motion
- 20 Calification
 20 DI trigger

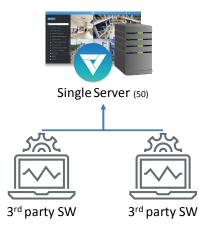
Rule:

The no. of licenses depends on how many alarm rules are using TCP Message as the triggering source.

Total no. of cameras: 32 Total instances of Alarm: 50 The no. of other triggering sources: 40 Needs 10 TCP Message licenses, and 0 for normal camera licenses (32 - 32).

NOTE: 32 camera channels are for free.

Calculation - Data Magnet License



Rule:

The no. of licenses depends on how many Data Magnet sources are implemented.

Total no. of Data Magnet sources: 2 Total no. of cameras: 50 Needs 2 Data Magnet licenses, and 18 normal camera licenses (50 - 32).

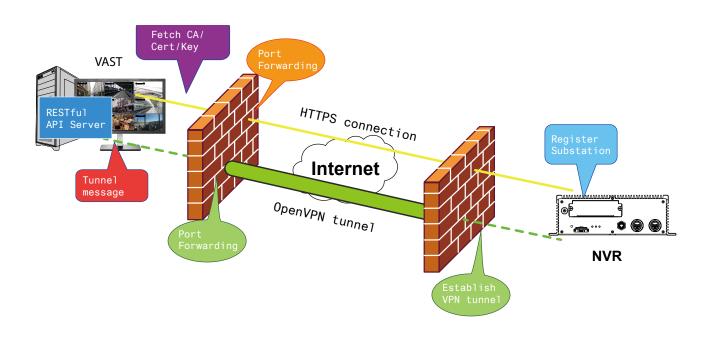
NOTE: 32 camera channels are for free.

Installation Option - OpenVPN

NAT-traversal with OpenVPN

You can select the "VAST Server with OpenVPN" option when installing the VAST server. A remote connection from NVR via a 3G/4G/LTE network can be made through an OpenVPN tunnel. When the OpenVPN option is selected, an OpenVPN server will be installed with the VAST server.

HMAC authentication and TLS encryption over an encrypted UDP connection are made effortlessly using the traversal methodology.



The sample installation screens are shown below:

VIVOTEK VAST2 Installation	VIVOTEK VAST2 Installation
Select the programs you want to install	V Installing
Server Server only Server with OpenVPN Client	Extract: openssl.exe 100%
Space required: 1009 MB	
< Back Next > Cancel	< Back Next > Cancel

The NVR runs an OpenVPN client that makes remote connection via the RESTful (Repretational State Transfer) API (Application Programming Interface) service to a VPN-enabled VAST server running on the remote site. The applicable service port number ranges from 1 to 65534. The default is port #3443. The NVR automatically registers with CA cert key and becomes a VAST sub-station over a VPN tunnel. Once set, the VAST2 can automatically connect the NVR.

Note that on the side of the VAST server making connection via the OpenVPN, the server/client configuration should be properly configured. On the mobile NVR, a proper gateway setting should be made for VPN connection.

For the server configuration, the configuration file is placed in: C:\Program Files (x86)\VIVOTEK Inc\VAST\Server\OpenVPN\config\server\server.ovpn

You can edit your VPN IP subnet parameters according to your network configuration. The contents of the editable text file looks like this:

port 3939 proto udp dev tun ca ca.crt cert server.crt key server.key dh dh.pem server 10.6.0.0 255.255.0.0 topology subnet client-to-client client-config-dir "C:\\Program Files (x86)\\VIVOTEK Inc\\VAST\\Server\\OpenVPN\\ccd" keepalive 10 30 cipher AES-256-CBC max-clients 50000 persist-key persist-tun status openvpn-status.log log-append openvpn.log verb 3 mute 20 sndbuf 262144 rcvbuf 262144 tls-server

Note that the NVR and VAST server should have a similar time setting when exchanging certificate information. Otherwise, the mutual handshake authentication process may fail.

Enter the OpenVPN DNS domain name and the credentials on the NVR network service configuration page.

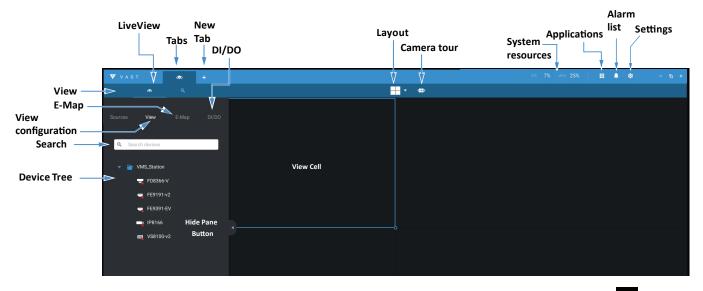
A public IP or domain name must be configured on the VAST server for the access through the Internet. The IP or domain name can contain alpha-numeric characters [0-9][a-z][A-Z][-]. [-] can not be the beginning or the ending character.

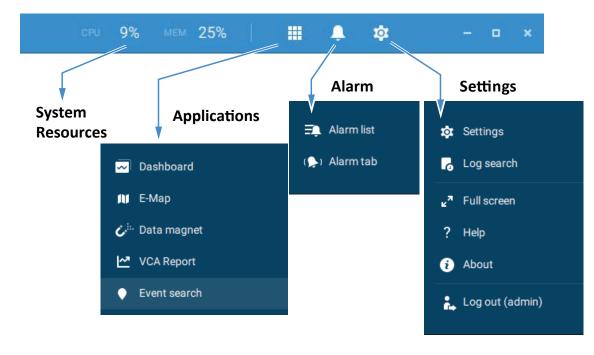
6)		Service port							
\$	нттр		1	80					
-		HTTPS		443					
		RTSP		554					
		CMS & iViewer							
_	✓ Allow access								
-		Port VAST 8		Viewer		3454			
·		VAST2 (same		5 HTTPS)		443			
		CMS Set up		assword for VAST & V	AST2	Reset passw	vord		
۲	IP		VAS	T2 remote connection	n				
4	DDNS	IP			nv9411p	.dnset.com			
		A		service port	3443		VAST2	1	
i	Service			rname ministrator)	admin			-	
È		Ac		ount password	•				
								Apply	

Chapter 2-1 Basics: Control and Elements

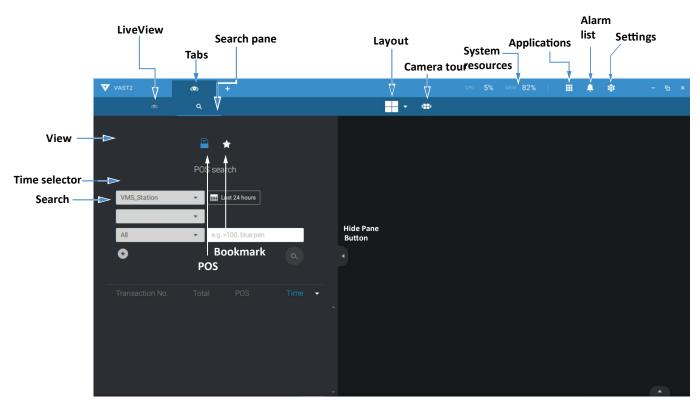
The basic screen elements of VAST live view, playback, and search pane are shown below:

Live view



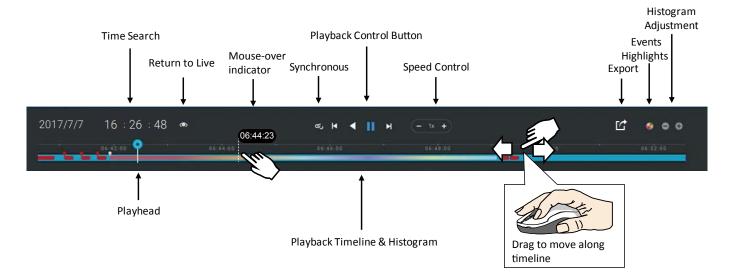


Top Tool Bar



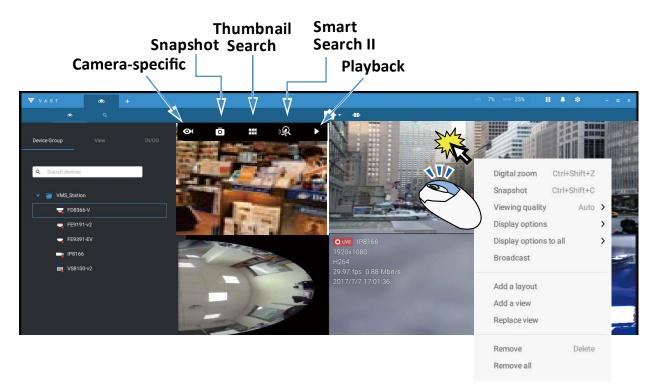
Search Pane

Playback Control



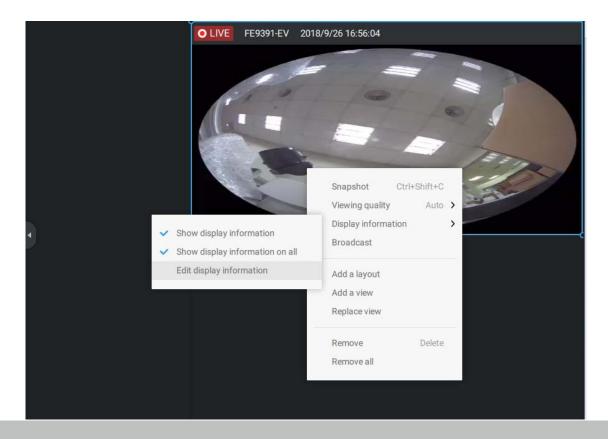
View cell control

Some controls and functions are available when a view cell is selected or via the right-click menus.



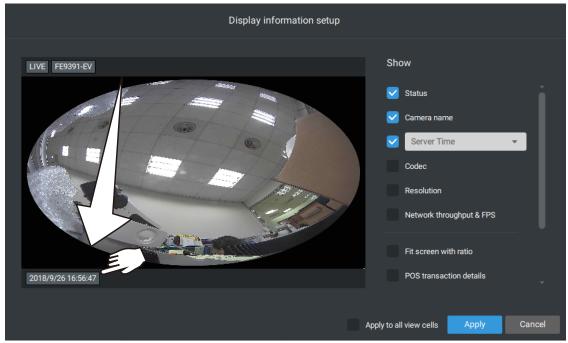
Text overlay

Single-click to select a view cell, right-click and select Display information. The Edit display information tab will appear.



Select the checkboxes to determine what kind of text overlay will display on view cells. Note that you can place the overlay either on top or at the lower screen. Simply click and drag an overlay item to a preferred location. When done, click the Apply button.

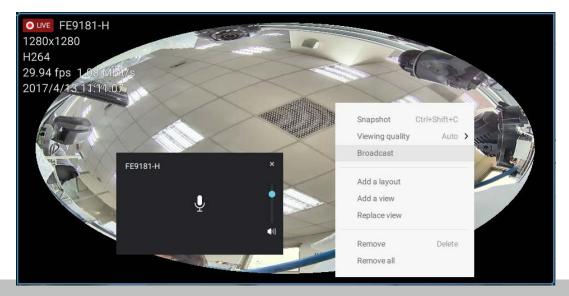
You can apply your current configuration to all view cells by selecting the **Apply to all view cells** checkbox. Note that you can also display the VCA rules and areas on screen.



Two Way Audio

If your cameras support the Two Way Audio feature and the microphone and audio output to an amplified speakers have been connected, you can right-click on the camera to display the Broadcast function. Click on the Microphone icon in the middle to start speaking. Click again to stop the Two Way Audio.

Note that the Broadcast option only appears when you select a camera that supports the Two Way Audio feature. Currently the VAST2 software supports 1 to 1 broadcast.



74 - User's Manual

Full Screen

The full screen function maximizes the display of view cells, concealing all other tool bar or navigation panels. To return to the normal view, press the **ESC** key on keyboard.

Log Search

System logs can be found via the tool bar tab. All system events will be listed in the Log search panel. If you have multiple server, substations, select a server. You can search specific events by the event types (All triggers, camera, system/site, external devices), or by the time of occurrence using the calendar tool.

Use the Export button it to export the system log as an individual log file.

💙 VAST2 💿 🌄 +					CPU 7% MEM 25% 🏭 🌲 🏟 – 🗆 ×
Log Search	17 results				Ľ
Select stations					Description
Q Search stations	1 2018/06/25	14:25:34 Event	Camera event - Camera connected to the ser	rver	Target camera name=FE9180-H
	2 2018/06/25	14:25:33 Operation	Camera management - Insert camera	server	New camera name=FE9180-H, New address=192.168.5.122, New port=80, New MAC=0002D1687
	3 2018/06/25	14:25:33 Operation	Recording - Update recording schedule	server@CMS	Schedule name=Default Schedule
i VMS_Station	4 2018/06/25	14:25:33 Operation	Recording - Insert recording schedule	server@CMS	Schedule name=VAST2 Default Continuous Recording
	5 2018/06/25	14:25:31 Operation	Camera management - Insert camera	server	New camera name=IP9191-HT, New address=192.168.5.104, New port=80, New MAC=0002D16B
	6 2018/06/25	14:25:31 Event	Camera event - Camera connected to the ser	rver	Target camera name=IP9191-HT
	7 2018/06/25	14:25:31 Operation	Camera management - Insert camera	server	New camera name=IB8377-HT, New address=192.168.5.112, New port=80, New MAC=0002D16A
	8 2018/06/25	14:25:31 Event	Camera event - Camera connected to the ser	rver	Target camera name=IB8377-HT
	9 2018/06/25	14:25:30 Operation	Recording - Delete recording path	server@CMS	Storage group name=DefaultGroup, Path=D:\recording
	10 2018/06/25	14:25:30 Operation	Recording - Insert recording path	server@CMS	$\label{eq:storage} Storage \ group \ name=DefaultGroup, Path=G:\Recordings, Reserve \ space=1024 \ MB$
· · · · · ·	11 2018/06/25	14:24:43 Operation	Login/out - Login	admin	User account=admin, Address=127.0.0.1
Select time frame	12 2018/06/25	14:22:56 System	System status - Server start		Service name=VAST Configuration Server
III Last hour	13 2018/06/25	14:22:56 System	System status - Server start		Service name=VAST Recording Server
Category	14 2018/06/25	14:22:55 System	System status - Server start		Service name=VAST Query Server
All	15 2018/06/25	14:22:53 System	System status - Server start		Service name=VAST Darwin Streaming Server
	16 2018/06/25	14:22:52 System	System status - Server start		Service name=VAST Event Server
Log type	17 2018/06/25	14:22:50 System	System status - Server start		Service name=VAST Backup Server
All					
Severity					

Log Level

Minor : Level 6~8 Normal : Level 3~5 Major : Level 1~2

Operation

VAST2 Type	Log Type	D	Level	Sample	Extra Parameters								
Login/out	Login	1	1	3 User Account=admin, Address=127.0.0.1	User account	Address							
	Logout	2	1	3 User Account=admin, Address=127.0.0.1	User account	Address							
User	Insert user	101	4	4 New User Name=guest, New Role=PowerUser, New	New User Name	New Role	New						
				Permission=000F01013F0201070307FFF6F77EFD4E00			Permission						
	Update user	104	:	5 Target User Name=guest	Target User Name								
	password												
	Update user	105	:	5 Target User Name=guest, Target Role=PowerUser, Target	Target User Name	Target	Target	New User	New Role	New			
	privilege			Permission=000F01013F0201070307FFF6F77EFD4E00,		Role	Permission	Name		Permission			
				New User Name=guest, New Role=PowerUser, New									
				Permission=000F01013F0201070307FFF6F77EFD4E00									
	Delete user	106	-	3 Target User Name=guest	Target User Name								
	Update user	107	-	5 Target User Name=guest	Target User Name								
	expiration												
Site	Insert station	201	4	4 New Station Name=VMS_Station, New	New Station Name	New	New Port	New	New RTSP	New Station			
				Address=172.18.60.31, New Port=3454, New UseSSL=0,		Address		UseSSL	Port	ID			
				New RTSP Port=3454, New Station									
				ID=S_{6312FAC9-FCF4-4573-964D-5F03D083BE54}									

	Update station information	202	Nam	et Station e={6312FAC9-FCF4-4573-964D-5F03D083BE54}, et Address=172.18.60.31, Target Port=3454, Target	Target Station Name	Target Address	Target Port	Target UseSSL	Target RTSP Port	New Station Name	New Address	New Port		New RTSP Port		
			Nam New	SSL=0, Target RTSP Port=3454, New Station e={6312FAC9-FCF4-4573-964D-5F03D083BE54}, Address=172.18.60.31, New Port=3443, New SSL=1, New RTSP Port=3443												
	Update station name	203		et Station Name=VMS_Station, New Station e=CMS	Target Station Name	New Station Name										
	Delete station	204			Target Station Name	Target Station ID										
	Set relay settings	1716	5 Enab	ole=true	Enable											
	Station enable multicast	2416	5 Stati	on name=VMS_Station	Station name											
	Station disable multicast	2417	5 Stati	on name=VMS_Station	Station name											
Camera	Insert camera	205	New	Camera Name=Door, New Address=172.18.1.129, Port=80, New MAC=0002D11CC24E, New HTTPS =443, New Recording Stream=1	New Camera Name	New Address	New Port	New MAC		New Recording Stream						
	Update camera information	206	Targ HTT	et Camera Name=Door, Target Address=172.18.1.129, et Port=80, Target MAC=0002D11CC24E, Target PS Port=443, Target Recording Stream=1, New Camera ue=IP8362, New Address=172.18.1.129, New Port=80,	Target Camera Name	Target Address	-	Target MAC	Target HTTPS Port	Target Recording Stream	New Camera Name	New Address	New Port	MAC	New HTTP S Port	New Reco rding Strea

			New MAC=0002D11CC24E, New HTTPS Port=443, New Recording Stream=1								m
	Delete camera	208	3 Target Camera Name=IP8362	Target Camera Name							
	Set digital output	701	4 Target Camera Name=IP8362	Target Camera Name							
	Set DI/DO name	1715	5 Target Camera Name=IP8362, Target Device=, Reference Name=Alarm	Target Camera Name	Target Device	Reference Name					
	Enable multicast	2414	5 Camera name=SD8362	Camera name							
	Disable multicast	2415	5 Camera name=SD8362	Camera name							
I/O device	Insert External Device	1151	4 Device Name=ADAM-6052, Device Host=172.18.60.70, Device Port=502	Device Name	Device Host	Device Port					
	Remove External Device	1152	3 Device Name=ADAM-6052, Device Host=172.18.60.70, Device Port=502	Device Name	Device Host	Device Port					
	Update External Device	1153	5 Device Name=ADAM-6052, Device Host=172.18.60.70, Device Port=502	Device Name	Device Host	Device Port					
	Set digital output	1154	2 Device Name=ADAM-6052, DO Index=8, Status=Trigger	Device Name	DO Index	Status					
Recording	Manually begin recording	301	2 Target Camera Name=IP8362	Target Camera Name							
	Manually	302	2 Target Camera Name=IP8362	Target Camera							

stop				Name							
recording Set recording	401	4	Storage Group Name=Office	Storage Group			 		 	 	-
storage				Name							
Insert recording schedule	402	4	Schedule Name=Working Time	Schedule Name							
Update recording schedule	403	5	Schedule Name=Working Time	Schedule Name							
Delete recording schedule	404	3	Schedule Name=Working Time	Schedule Name							
Insert storage group	411	4	Storage Group Name=Office, Cycle=True	Storage Group Name	Cycle						
Update storage group	412	5	Storage Group Name=Office, Cycle=True	Storage Group Name	Cycle						
Delete storage group	413	3	Storage Group Name=Office	Storage Group Name							
Insert recording path	414		Storage Group Name=Office, Path=E:\recording, Reserve Space=90112 MB	Storage Group Name	Path	Reserve Space					
Update recording path	415		Storage Group Name=Office, Path=E:\recording, Reserve Space=102400 MB	Storage Group Name	Path	Reserve Space					
Delete recording	416	3	Storage Group Name=Office, Path=E:\recording	Storage Group Name	Path						

	path										
	Insert camera to the storage group	417	4 Storage Group Name=Office, Camera Name=IP8362	Storage Group Name	Camera Name						
	Delete camera from the storage group	419	3 Storage Group Name=Office, Camera Name=IP8371E	Storage Group Name	Camera Name						
Network	Update server port	1701	5 Server Name=Web, Port=3455	Server Name	Port						
	Set proxy server	1702	5 Enable=True, Address=172.18.60.13, Port=80	Enable	Address	Port					
	Set UPnP	1703	5 UPnP Port Forwarding Enable=False, UPnP Presentation Enable=True	UPnP Port Forwarding Enable	UPnP Presentatio n Enable						
	Set DDNS server	1704	5 Enable=True, Provider= <u>Dyndns.org</u> (Dynamic)	Enable	Provider						
Alarm	Insert alarm management	408	4 Alarm name=alarm, Trigger list=Motion detection - Motion window 1 of Network Camera, Action list=Set DO status - DO-1 of Network Camera	Alarm name	Trigger list	Action list					
	Update alarm management	409	5 Alarm name=alarm, Trigger list=Motion detection - Motion window 1 of Network Camera, Action list=Set DO status - DO-1 of Network Camera	Alarm name	Trigger list	Action list					
	Delete alarm management	410	3 Alarm name≕alarm	Alarm name							
	Stop alarm sound	2408	7 Alarm name=alarm	Alarm name							

	Close alarm notification panel	2409	7 Alarm name=alarm	Alarm name							
	Mute alarm	2411	7 Alarm name=alarm, Duration=10mins,	Alarm name							
PTZ	Camera PTZ,	702	7 Target Camera Name=SD9361-EH	Target Camera							
	Iris, Focus,			Name							
	Pan, Patrol										
	control										
	Click on	703	7 Target Camera Name=SD9361-EH	Target Camera							
	image			Name							
	Select preset	704	7 Target Camera Name=SD9361-EH, Preset Name=Door	Target Camera	Preset						
	location			Name	Name						
Backup	Update	1503	5 Enable=true	Enable							
	scheduled										
	backup										
License	Update	1717	5 (Empty)								
	license										
	information										
System	Create	1705	4 Target Path=E:\test	Target Path							
	directory										
	Rename	1706	5 Source Path=E:\test, Target Path=E:\recording	Source Path	Target Path						
	directory										
	Delete	1707	3 Target Path=E:\recording	Target Path							
	directory										
	Update server	3401	3 Old path=E:\clientlogs, Target Path=E:\test								
	database path										
	Insert SMTP	1708	4 Target Address=mail.vivotek.tw, Target Port=25, Target	Target Address	Target Port	Target Order					

server		Order=0									
Update SMTP serv	1709 er	5 Target Address= <u>mail.vivotek.tw</u> , Target Port=25, Target Order=0, New Address= <u>mail.vivotek.com</u> , New Port=25, New Order=0	Target Address	Target Port	Target Order	New Address	New Port	New Order			
Delete SM [*] server	P 1710	3 Target Address= <u>mail.vivotek.tw</u> , Target Port=25, Target Order=0	Target Address	Target Port	Target Order						
Insert network storage	1711	4 Target Host=rd2fs, Target Domain=vivotek	Target Host	Target Domain							
Update network storage	1712	5 New Host=rd2fs, New Domain=vivotek, Target Host=rd2fs, Target Domain=vivotek	New Host	New Domain	Target Host	Target Domain					
Delete network storage	1713	3 Target Host=rd2fs, Target Domain=vivotek	Target Host	Target Domain							
Watermark settings	2418	5 Status=Disable Status=Enable	Status								
Import devi pack	ce 1721	4 Original version=xxxx, New version=000	Original version	New version							
Import devi pack failed	ce 1722	4 Reason=Invalid device pack Reason=Failed to import device pack	Reason								
Add camera	2402	7 New Camera(s) = C1, Total Camera(s) in View= C1,C2	New Camera(s)	Total Camera(s) in View							
Remove camera	2403	7 Removed Camera(s) = C1, Total Camera(s) in View= C2	Removed Camera(s)	Total Camera(s)							

					in View							
	Replace	2404	7 Removed Camera(s) = C1, New Camera(s) = C2,C3 Total	Removed	New	Total						
	camera		Camera(s) in View= C2,C3	Camera(s)	Camera(s)	Camera(s) in						
						View						
View	Add view	2401	5 View Name = View001, Add Camera(s) = C_1	View Name	Add							
					Camera(s)							
	Delete view	2405	5 View Name = View001, Removed Camera(s) = C_1, C_3	View Name	Removed							
					Camera(s)							
	Update view	2406	5 View Name = View001, Removed Camera(s) = C_3, Add	View Name	Removed	Add	Total					
			Camera(s) = C_1, Total Camera(s) in View= C_1, C_2		Camera(s)	Camera(s)	Camera(s)					
							in View					
	Rename view	2407	5 Old View Name = View001, New View Name = View002,	Old View Name	New View	Total						
			Total Camera(s) in View= C1, C_2		Name	Camera(s) in						
						View						
Data magnet	Add data	2601	4 Name=Lane, Port=1234, Camera name=FE8173	Name	Port	Camera						
	source					name						
	Update data	2602	5 Target name=Lane, Targe port=1234, Target camera	Target name	Targer port	Target	New name	New port	New camera			
	source		name=FE8173, New name=Lane, New port=4321, New			camera name			name			
			camera name=IP8362									
	Delete data	2603	3 Name=Lane	Name								
	source											
	Show data	2604	7 Enable=True, Camera name=FE8173	Enable	Camera							
					name							
EMap	Add EMap	3201	7 New EMap(s) = /Dessert, Total EMap(s) in View=	New EMap(s)	Total							
			/Dessert,/Penguin		EMap(s) in							
					View							
	Delete EMap	3202	7 Removed EMap(s) = /Dessert, Total EMap(s) in View=	Removed EMap(s)	Total							

				/Penguin		EMap(s) in View						
	Replace	3203	7	Removed EMaps(s) = /Dessert, New EMap(s) =	Removed EMap(s)	New	Total					
	EMap			/Flower,/Lion Total EMap(s) in View=/Flower,/Lion		EMap(s)	EMap(s) in					
							View					
VCA Report	Auto update	2801	5	VCA Chart Auto Update=true	VCA Chart Auto							
	report				Update							
	Auto update	2802	5	VCA Chart Update Frequency=999	VCA Chart Update							
	frequency				Frequency							
Matrix	Assign	3001	7	User=admin, assign component=Google map, to	User name	Component	Client name	Screen ID				
	component			client=WIN-458HOD557IM, screen=1								
	Reset all	3002	7	User=admin, reset all screen to client=WIN-458HOD557IM	User name	Client						
						name						
PPTZ	PPTZ	2410	7	Enable=True, Camera name=FE8173								
	Control											

Event

VAST2 Type	Log Type	D	Level	Sample	Extra Parameters
Camera	Camera disconnected from	1101	2	Target Camera Name=SC8131	Target Camera Name
	server				
	Camera connected to the	1102	2	Target Camera Name=SC8131	Target Camera Name
	server				
System	Parent station disconnected	1201	2	Target Station Name=VMS_Station	Target Station Name
	Parent station connected	1202	2	Target Station Name=VMS_Station	Target Station Name
	Parent station connection lost	1203	2	Target Station Name=VMS_Station	Target Station Name

	Parent station connection restored	1204	2 Target Station Name=VMS_Station	Target Station Name					
	Substation disconnected	1205	2 Target Station Name=NV9411P	Target Station Name					
	Substation connected	1206	2 Target Station Name=NV9411P	Target Station Name					
	Substation connection lost	1207	2 Target Station Name=NV9411P	Target Station Name					
	Substation connection restore	1208	2 Target Station Name=NV9411P	Target Station Name					
	Start scheduled backup	1501	2 Backup Path=E:\backup, Backup Interval=2018/02/05 00:00:01-2018/02/06 23:58:40	Backup Path	Backup Interval				
	Stop scheduled backup	1502	2 Backup Result Desc=Backup Finish, Backup Interval=2018/02/05 00:00:01-2018/02/06 23:58:40, Backup Latest End Time=2018-02-06 23:58:40.506	Backup Result Desc	Backup Interval	Backup Latest End Time			
	Schedule backup error	1504	2 Media File Source Path=D:recording\2018-02-04\2-SC8131\1_ 2018-02-04_000001.3gp, Backup Destination Path=E:\backup, Reason=source is not exist	Media File Source Path	Backup Destination Path	Reason			
Alarm	Alarm trigger	1601	2 Alarm Name=Test, Trigger Type=DO, Action Type=Start to record on	Alarm Name	Trigger Type	Action Type			

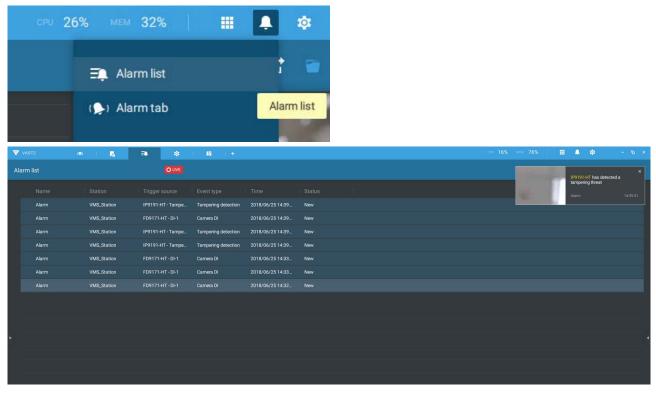
System

VAST2 Type	Log Type	D	Level	Sample	Extra Parameters
System	Server start	1001	1	Service Name=VAST Configuration Server	Service Name

Server stop	1002	1	Service Name=VAST Configuration Server	Service Name					
Trial expired	1003	1	(Empty)						
Key dongle lost	1004	1	(Empty)						
Virtual memory low	1005	1	(Empty)						
Network lost	1006	1	(Empty)						
Camera MAC invalid	1007	1	(Empty)						
License invalid	1008	1	Invalid Item=Number of VIVOTEK camera(s) exceeded	Invalid Item					
Storage lost	1602	2	Path=Volume1	Path					
Failover start	2301		Active Station Name=CMS, Active Station ID=S_{f2725102-d790-4bbb-9f27-ab10356b55bd}, Redundant Station Name=NVR, Redundant Station ID=S_{50ef2623-7143-50d2-9e09-7552798e0e2b}	Active Station Name	Active Station ID				
Failover stop	2302		Active Station Name=CMS, Active Station ID=S_(f2725102-d790-4bbb-9f27-ab10356b55bd), Redundant Station Name=NVR, Redundant Station ID=S_(50ef2623-7143-50d2-9e09-7552798e0e2b}	Active Station Name	Active Station ID				
Start NVR backup	2412	2	Station name=NVR, Reason=Backup triggered	Station name	Reason				
Stop NVR backup	2413	2	Station name=NVR, Reason=Backup Finished	Station name	Reason				

Alarm list

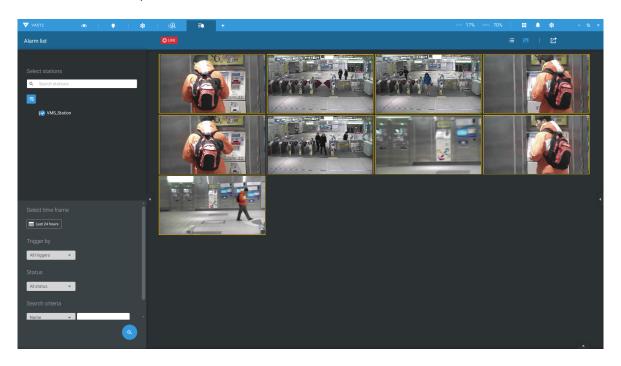
The Alarm list is accessed from the top tool bar. The Alarm list provides easy access to all triggered alarms, such as tampering alarms, alarms reported by VCA analytics, external devices connected via a camera's DI pin, etc.



The Alarm list can be displayed in either the List view or Thumbnail view.

CPU 26%	мем 32% 📔 🔛	\$ \$ − □ ×
	iiii 🛄 🛄	L
	List view ↓ E: Thumbnail view	xport ↓ Export target folder

Below is an example of a Thumbnail view.



On the Alarm list, you can double-click to select a triggered alarm. A related snapshot and configuration panel will appear. An operator can select the Status menu to change the event management status. The configurable statuses can be:

- 1. New: An event that has not been handled.
- 2. In progress: Select to indicate that the event is being handled, e.g., a security personnel has been sent to verify the cause of the event.
- 3. False alarm: Used to indicate the event has been verified as a false alarm.
- 4. Close: A closed case event will be erased from the event list.

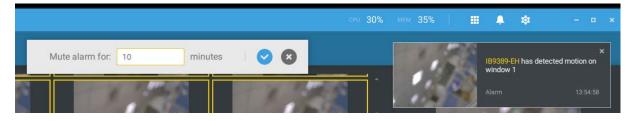
When done with designating event status, click the Acknowledegment button.

VAST2	• <mark>6</mark>	3 . Ø	16 +			6		\$	
Alarm list		OLIVE						Ľ	
Alarm	VMS_Station	IP9191-HT - Tampe	Tampering detection	2018/06/25 14:39	New				
Alarm	VMS_Station	IP9191-HT - Tampe	Tampering detection	2018/06/25 14:39	New				
Alarm	VMS_Station	FD9171-HT - DI-1	Camera DI	2018/06/25 14:39	New				
Alarm	VMS_Station	IP9191-HT - Tampe	Tampering detection	2018/06/25 14:39	New				
Alarm	VMS_Station	IP9191-HT - Tampe	Tampering detection	2018/06/25 14:39	New	Alarm			
Alarm	VMS_Station	FD9171-HT - DI-1	Camera DI	2018/06/25 14:33	New	VMS_Stat	on		
Alarm	VMS_Station	FD9171-HT - DI-1	Camera DI	2018/06/25 14:33	New	IP9191-H	- Tamperi	ng	
Alarm	VMS_Station	FD9171-HT - DI-1	Camera DI	2018/06/25 14:32	New	Status	In progre	SS	
							New In progre	200	
							False ala		
							Close	0	
							Ackn	owledgm	nent

The Alarm list also supports Hot keys.

Alarm list window			
Mute the current alarm	Ctrl		m
Designate the selected alarms	Ctrl		f
as false alarms			
Select all alarms	Ctrl		а
Select one or multiple alarms	Ctrl		left mouse button
Select multiple alarms		Shift	left mouse button
Select different alarms			Up/Down/Left/Right

When an alarm is muted, a message will prompt asking for how long the alarm will be muted. Enter a number, and the alarm will disappear from the list temporarily.



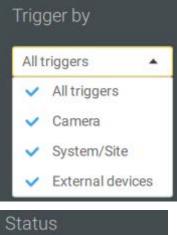
When an alarm is designated as a false alarm, it is immediately removed from the list.

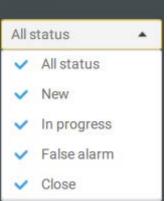
When an alarm is designated as In progress, you can add a comment on the current condition, and click Acknowledge to change its status.

ID9309-EH - WINDOW I	Wotion detection	2010/12/22 14:00:20	New	
IB9389-EH - Window 1	Motion detection	2018/12/22 14:04:59	New	100 B 100
IB9389-EH - Window 1	Motion detection	2018/12/22 13:49:42	New	< 1/2 ▶
IB9389-EH - Window 1	Motion detection	2018/12/22 13:48:29	New	Alarm
IB9389-EH - Window 1	Motion detection	2018/12/22 13:48:18	New	VMS_Station
IB9389-EH - Window 1	Motion detection	2018/12/22 13:48:09	New	IB9389-EH - Window 1
IB9389-EH - Window 1	Motion detection	2018/12/22 13:48:04	In progress	Status In progress -
IB9389-EH - Window 1	Motion detection	2018/12/22 13:47:37	New	History
IB9389-EH - Window 1	Motion detection	2018/12/22 13:46:58	New	
IB9389-EH - Window 1	Motion detection	2018/12/22 13:45:35	New	Ω.
IB9389-EH - Window 1	Motion detection	2018/12/22 13:45:10	New	
IB9389-EH - Window 1	Motion detection	2018/12/22 13:45:00	New	
IB9389-EH - Window 1	Motion detection	2018/12/22 13:41:52	New	one sent to verify
IB9389-EH - Window 1	Motion detection	2018/12/22 13:41:21	New	
IB9389-EH - Window 1	Motion detection	2018/12/22 13:41:10	New	Acknowledge

×







To find alarms of specific types, time of occurrences, and alarm status, click the side tab to reveal the search panel.

You can select the trigger source, e.g., when you need to see camera alarms only.

You can check to see alarms of a specific status. For example, you can select to search for the "In progress" alarms only.

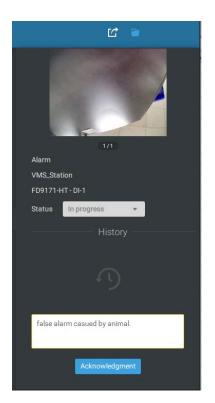
Search crite	ria		
Name	Ŧ	Ala	0
Name	•		•

You can enter one or multiple keywords as the search criteria.

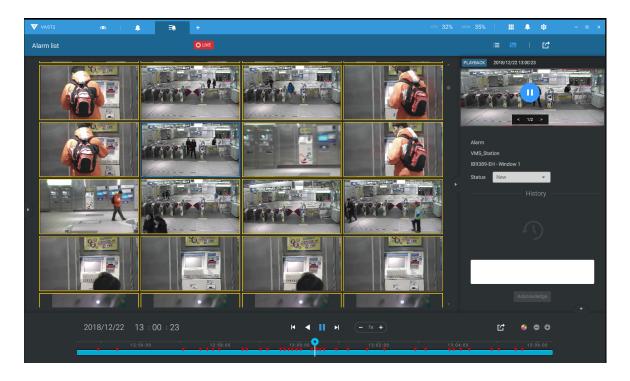
For example, if you have an alarm named as "Alarm3-sidewalk," use the name as the keyword to search for the related alarms.

You can use the Export button for export a full list of all triggered events into a CSV file. The event type, receiving station, triggering device, time of occurrence, and event status will all be listed. You can also export alarm-triggered videos.

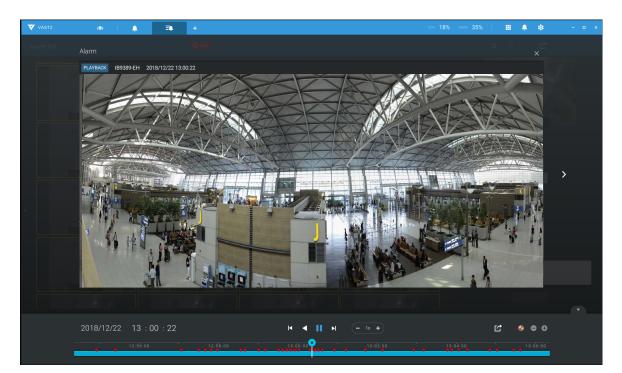
You can also add a comment for an event by entering the description in the comment entry field.



To review the alarm-related video, click to select an alarm, double-click to playback. The Playback window will appear on the upper right of the screen.

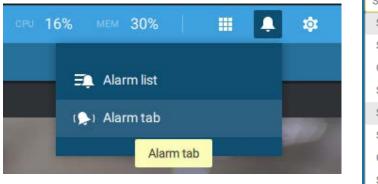


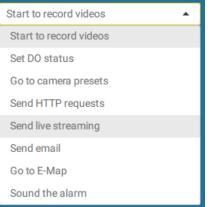
Double-click on the small playback screen again to bring it to the full view. The playback control, time line, export, and alarm tags will be available on screen.



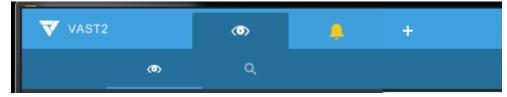
Alarm tab

The Alarm tab is an automated streaming window displaying live videos by the triggered alarms. If you configure an alarm action as "Send live streaming," the alarm streaming will be displayed in this window. Note that this window does not display other alarms.





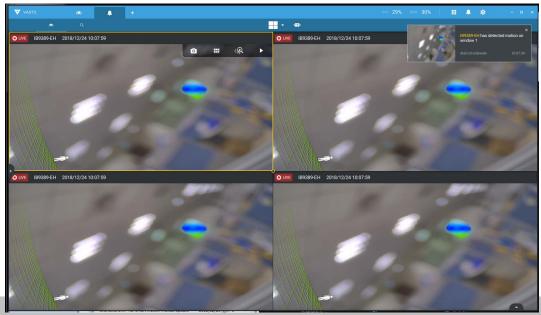
When a live streaming is sent with an alarm, an orange ringing bell icon will displays.



An alarm prompt will also display on the screen.



You can click on the ringing bell icon to open the Alarm tab window. The alarm-trigged streamings will be available on screen.



88 - User's Manual

Hot Keys

Open online document			F1
Close current tab	Ctrl (Win) /		W
	Command (MacOS)		
Open new Live / Playback tab	Ctrl (Win) /		Т
	Command (MacOS)		
Full screen	Ctrl (Win) /	Shift	F
	Command (MacOS)		
Exit full screen	Ctrl (Win) /	Shift	F
	Command (MacOS)		
Exit full screen			Esc
View cell			
Select view cell			Arrow keys
Digital zoom	Ctrl (Win) /	Shift	Z
	Command (MacOS)		
Snapshot	Ctrl (Win) /	Shift	С
	Command (MacOS)		-
Instant bookmark	Ctrl (Win) /	Shift	В
	Command (MacOS)		
Remove camera from cell	,		Del
Move to preset position	Ctrl (Win) /		Digits (1,2,3,)
	Command (MacOS)		J ²² () , ² , ⁷
PTZ model up, down, left, right	· · · · · · · · · · · · · · · · · · ·		Arrow keys
Save current layout as a	Ctrl (Win) /		S
customized layout	Command (MacOS)		
Undo layout modification	Ctrl (Win) /		Z
,	Command (MacOS)		
Redo layout modification	Ctrl (Win) /		Y
ç	Command (MacOS)		
	, , , , , , , , , , , , , , , , , , ,		
Timeline			
Sync Playback mode	Ctrl (Win) /	Shift	S
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Command (MacOS)		
Pause (Play/Rewind)	, , , , , , , , , , , , , , , , , , ,		Space
Play	Ctrl (Win) /		Arrow right
,	Command (MacOS)		5
Rewind	Ctrl (Win) /		Arrow left
	Command (MacOS)		
Speed up	Ctrl (Win) /		Up
	Command (MacOS)		.
Speed down	Ctrl (Win) /		Down
	Command (MacOS)		
Next frame	, , , , , , , , , , , , , , , , , , ,	Shift	Arrow right
Previous frame		Shift	Arrow left
Reset speed to 1x	Ctrl (Win) /		1 (one)
•	Command (MacOS)		

Smart search II		
- Configuration page		
Delete detection range		Esc

Bookmark search			
Select more bookmarks	Ctrl (Win) /		Click
	Command (MacOS)		
Select more bookmarks		Shift	Click
Back to bookmark page			Esc
Next bookmark			Arrow right
Previous bookmark			Arrow left
Thumbnail search			
Select thumbnail			Arrow keys
Play a selected thumnail			Enter
Back to Thumbnail page			Esc
Next Thumbnail			Arrow right
Previous Thumbnail			Arrow left
Emap Setup			
- Google map			
Remove selected GPS			Del
DI/DO Device Settings			
Remove selected external I/O			Del
device			
SMTP Settings			
Remove selected SMTP			Del
server			
Camera Management			
Rename selected camera			F2
Rename selected folder			F2
Remove selected camera			Del
from system			
Sites Management			
Rename selected site		ļ	F2
Remove selected site from			Del
system			
Users Settings			Del
Remove selected user			Del
Schedule Settings			
Remove scheduled time frame			Del
			<u> </u>

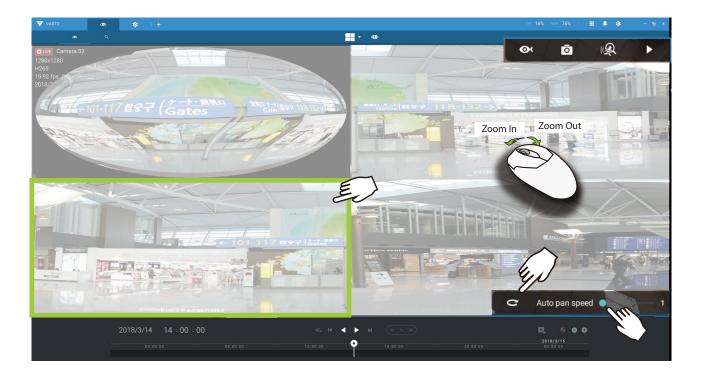
Data Magnat		1	
Data Magnet			
Move selected row			Up / Down
Show detail of selected row			Enter
View management			
Rename selected view			F2
Delete selected view			Del
Alarm management			
Delete selected alarm			Del
Alarm list window			
Mute the current alarm	Ctrl (Win) /		m
	Command (MacOS)		
Designate the selected alarms	Ctrl (Win) /		f
as false alarms	Command (MacOS)		
Select all alarms	Ctrl (Win) /		а
	Command (MacOS)		
Select one or multiple alarms	Ctrl (Win) /		left mouse button
	Command (MacOS)		
Select multiple alarms		Shift	left mouse button
Select different alarms			Up/Down/Left/Right

View Cell Elements

On a view cell, the control elements are different with different types of network cameras. 3 major types are listed below with applicable screen elements:

- 1. Fixed cameras: 🗖 🏾 🖗 🕨 Snapshot Thumbnail search Smart search Replay.
- 2. **Fisheye** cameras: Fisheye display mode Snapshot Thumbnail search Smart search Replay.

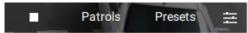
The Auto pan function applies only to the Regional views. Select a regional view, and click the Auto pan button. The Regional view will pan from side to side to cover more viewable regions. If a fisheye is mounted on wall, a regional view with auto pan can cover a panoramic view region.



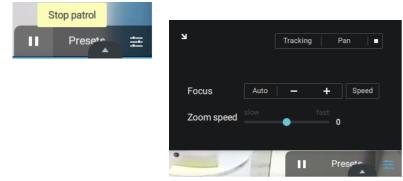
3. **PTZ** cameras: Search - Replay. For information about PTZ control, refer to the discussion on PTZ on page 136.

To exert PTZ control, first click on this button to enable PTZ control.

When PTZ control is enabled, the following controls are available on screen:



Click Patrols or Presets if these have been configured on the PTZ camera. You will need to open a web console with the camera to do so.



The PTZ settings tab allows you to enable PTZ Tracking and the Pan functions. You can also adjust the Zoom and Focus speed, or manually adjust the focus. Please refer to the camera User Manual for more information about these functions.



For speed dome cameras that comes with wiper blade, the wiper blade control button will be available on the tool bar.

You can use the mouse wheel to zoom in or zoom out on the screen. The zoom ratio is shown on screen for half a second.



When PTZ is enabled, the zoom buttons and a home button are displayed on the right hand side of the view cell.

For more information about Snapshot, Thumbnail search, and the Replay functions, please refer to their specific help pages.

ō -----(Q) Enable Optical - Snapshot -3. Motorized lens cameras:

Thumbnail search - Smart search - Replay.

For cameras that come with motorized zoom lens, click on the Enable Optical button. You can zoom in or zoom out on the scene.

0	No. No.	A Design of the second second		N 10/2			
O LIVE FD938	37-HTV-A	2020/5/14 11:05:4	2				
		Motion	و ndow 1			(<u>Q</u>	•
		Enable	Optical		Zoom ir	1 –	+
					Zoom o	out	
	-			Focus ad	justment		- 2
						-	

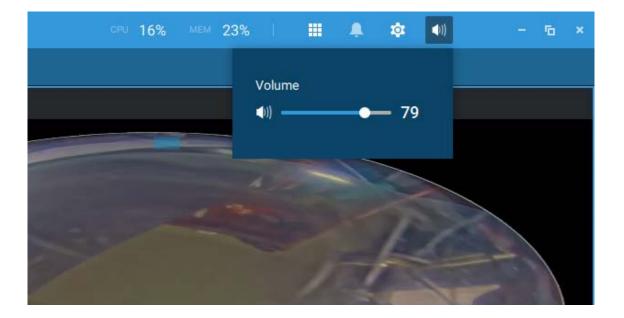
Click on the Focus adjustment button to bring out the focus panel. If you find the image is out of focus, you can use the +, -, or Auto buttons to regain the best image focus.

You can use the Auto scan function to let the camera automatically find the best focus. The process may take up to 20 seconds.

5/14 1	1:06:59					
	€	ō		<u>,</u>	►	
М	otion Window 1					
						+
	ч					
	Focus	Auto	-	+	Speed	
	Zoom speed	slow	•	fast 4		

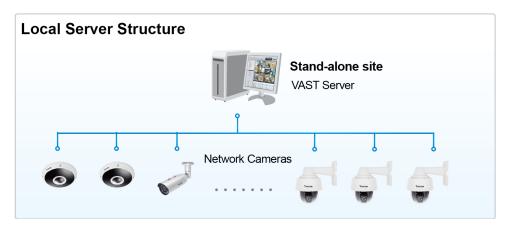
Audio

For a view cell housing a camera with an audio input, you can tune its volume using the slide bar on the tab panel.



VAST Server and Client Components

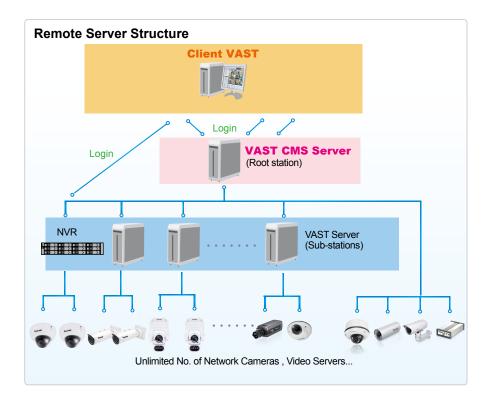
VAST2 Server provides a centralized management site for video recording. Users can login and modify the server's configuration, edit the server's recording storage, configure schedules and many other functions. You can browse the recorded video database and video clips related to specific events on the server.



For users who manage large-scale surveillance deployments, please plan the hierarchical structure first. Then you can start to add cameras to each station and connect these substations to the root station. The whole hierarchical management system is thus constructed. VIVOTEK's NVR stations can also be included as sub-stations. The Logical Tree view becomes the default.

Multiple Server Applications

A host with the VAST2 installed is recognized as a stand-alone site. All the functions can be simultaneously performed on one single site.



Please refer to the Sites page for how to enlist VAST sub-stations.

Minimum System Requirements

Before installing the VAST software, please make sure your system meets the following recommended minimum system requirements.

VAST2 Server			
Operating System	Windows 10, 7, Windo type is not supported		6 (Server core installation
Server (Recording Channels)	Up to 64 CH	Up to 128 CH	Up to 256 CH
CPU	6th Generation Intel® or above	Core™ i3 Processors	6th Generation Intel® Core™ i5 Processors or above
RAM****	4 GB or above	8GB or above	8GB or above
Hard Drive (Enterprise model only), suggestion	1 Volume Group*	2 Volume Group*	4 Volume Group*
Recording throughput	1 Volume Group: Max	. 200Mbps (Max.)**	
Network Interface Card	Ethernet, 1Gbit recom	imended***	

- * The size of volume group depends on the total recording server throughput.
- ** The maximum combined bit rate of cameras cannot exceed the total recording throughput.
- *** Please consider the combined throughput of viewing, recording, and server's network bandwidth when designing your surveillance deployments.
- **** Please use a dual-channel memory configuration.

VAST 2 Liveview & Playback							
Operating System		Windows Server 2012, 2016 / Windows 10, 7 / MacOS 10.15 Catalina (Server core installation type is not supported.)					
Clients	720P,2Mbps, H.264,* each CH	8 CH	16 CH	32 CH			
(Display Channels)	1080P,4Mbps, H.264**, each CH	6 CH	10 CH	18 CH			
Channels)	1080P,4Mbps, H.265, each CH	3 CH	5 CH	9 CH			
CPU		6th Generation Intel® Core™ i3 Processors	6th Generation Intel® Core™ i5 Processors	6th Generation Intel® Core™ i7 Processors			
RAM***		8GB or above	8GB or above	16GB or above			
Network Int	erface Card	Ethernet, 1Gbit recommended					
Graphics Ca	ard****	Direct3D acceleration with 1GB RAM graphics card					

* Each recording group can receive recordings for 60 channels.

- * Display requirements of the 3MP fisheye camera is equal to a 720P camera.
- ** Display requirements of the 5MP fisheye camera is equal to a 1080P camera.
- *** Please use a dual-channel memory configuration.

**** Please update to the lastest GPU driver.

If you plan to install both VAST2 server and client on the same computer, please remember to consider the combined load on computing, encode/decode effort, and bandwidth.

The 60-day trial includes 256 channel license and all advanced license features.

The required hard disk space will depend on the video settings, the number of network cameras and recording group settings. Please add more hard disks if you want to extend the system.

Below are the approximate numbers for a week-long recording. The actual storage space required also depends on imaging parameters, e.g., a complex retail environment that involves many moving objects requires more pixel data to be transmitted over network than a simple environment such as a parking lot. The following numbers are based on H.264 recording.

32-CH, VGA, about 1 week recording: 750 GB
64-CH, VGA, about 1 week recording: 1TB x 2
32-CH, 2-megapixel, about 1 week recording: 2TB x 2
64-CH, 2-megapixel, about 1 week recording: 2TB x 4

Chapter 2-2 Starting Up

Double-click the VAST2 icon vast2 on the desktop to start the VAST2 main page.

When started the first time, the server automatically polls the local network for reacheable network cameras. For cameras that come with pre-configured User Name and Passwords, the server prompts for entering credentials for the access to cameras. Check out the cameras' MAC addresses to identify the cameras.

The cameras found within the network will be listed. If the need should arise, you can use the Search panel on top to locate specific cameras using their IP, MAC, Port, Model name, or brand name (ONVIF/VIVOTEK).

Use the 📕 Add device button to manually add a camera with its known IP or domain name.

Use the Import Device List button to recruit cameras in a previously-saved device list (CSV files).

Use the Authorize button if the camera found in the Search panel needs credentials.

When search is done, delete the alpha-numeric characters in the search field to return to the device list.

Use the Refresh 💿 button to search the local network again.

			anan a			- 15 ×	
			Add device				
						Authorize 3 selected device	
O .,	Add 15 device(s)						
Add device	Q IP, MAC, Port, Model, Brand (or	nvif/vvtk) Authorize	+ 5		4	192.168.4.150	>
	Status IP	- MAC	Port Model	Brand		00-02-D1-5F-E7-24	
	192.168.6	.101 00-02-D1-4B	×				
	192.168.6	.103 00-02-D1-49	Authorize 3 selected devices				
	192.168.6	.104 00-02-D1-4C				root	
	192.168.6	<	≠ 192.168.6.107 00-02-01-20-1A-BC >				
0	192.168.6		• 00-02-01-20-1A-BC	ONAIL			
Ready to use	192.168.6	and the second the	User name			•••••	
	192.168.6	.126 00-02-D1-28	Poste mente				
	192.168.6	.129 F0-7D-68-0F	Password	ONVIF			
	192.168.6	.131 00-02-D1-4B					
	192.168.6	.143 B0-C5-54-06	Amm nill Cancel	ONVIS		Apply all	Cancel
					Next Cancel		
-							

2-2-1. Selecting Devices

Use the checkboxes in front of the listed devices to determine which devices will be recruited to your configuration. By default, all cameras are selected. When the selection is done, click on the Next button at the lower right screen.

If any of the selected devices requires credentials, the authorization window will prompt.

NOTE:

For cameras that come without a password protection, you should open the Shepherd utility to locate and open a web console, and configure a password for protecting the access to the camera. If a brand new camera (with no password) is selected for your VAST configuration, it will join your configuration without the password protection.

			Language
FD9181-HT			
Configure password At least 8 characters with no space, one character(uppercase or lowercase), and character			
User name :	root		
User password :	•••••	Medium	
Confirm user password :	•••••]	
	 Enable https connect configuration for pass 		
*The new password will be applied to all	connections		
	Sa	Cancel	

2-2-2. Recording Options

Click Settings > Recording > Recording options. The Recording options window will prompt.

You can configure recording schedules or select the storage options, including the configuration of an external NAS storage.

V V A S T	o \$ +		n 🗠 🏘 🛔 ? – n ×
🔊 Settings	4	Recording options	
Recording options	VMS_Station	Archive name DefaultGroup Site VMS.Station	
Backup		Storage + New storage	Recycle Options
Failover		D.\recording G.\Recordings	
		5 cameras Select cameras	
		Name IP Streaming Schedule	Seamless recording Activity Adaptive Stream
		All cameras 🗸 🗸	
		FD8366-V 192.168.4.150 1 • Continuous •	
		FD8377-HV 192.168.4.171 1 v Continuous v	
		VS8100-v2 192.168.4.172 1 v Continuous v	
			Apply Cancel

Click on the Schedule column on the Camera list for a recording option: Continuous recordings, Events only, None, or Default Schedule, or New template. You can apply a schedule template for all cameras or configure individual schedules for different cameras. When using the Event-triggered recording, a pre-event and post-event time can be configured. An Edit pane is available by clicking the Edit \bigcirc button.

You can manually create a recording template using the **New template** option. When done, each configured template will be listed below.

imeras	Select cameras				
Name	IP	Streaming	Schedule		Seamless recording
All cameras			Schedule_work_hours	1	
FD8366-V	192.168.4.150	1 💌	New template	1	
FD8377-HV	192.168.4.171	1 💌	Event only Continuous	1	
VS8100-v2	192.168.4.172	1 💌	None	1	
FE9391-EV	192.168.4.178	1 💌	Default Schedule	1	
FE9191-v2	192.168.4.149	1 👻	Schedule_work_hours		
	Name All cameras FD8366-V FD8377-HV VS8100-v2 FE9391-EV	Name IP All cameras 192.168.4.150 FD8366-V 192.168.4.171 FD8377-HV 192.168.4.171 VS8100-v2 192.168.4.172 FE9391-EV 192.168.4.178	Name IP Streaming All cameras 1 1 FD8366-V 192.168.4.150 1 FD8377-HV 192.168.4.171 1 VS8100-v2 192.168.4.172 1 FE9391-EV 192.168.4.178 1	Name IP Streaming Schedule All cameras Schedule_work_hours FD8366-V 192.168.4.150 1 • New template FD8377-HV 192.168.4.171 1 • Continuous VS8100-v2 192.168.4.172 1 • None FE9391-EV 192.168.4.178 1 • Default Schedule	NameIPStreamingScheduleAll camerasSchedule_work_hoursFD8366-V192.168.4.1501New templateFD8377-HV192.168.4.1711ContinuousVS8100-v2192.168.4.1721NoneFE9391-EV192.168.4.1781Schedule_work_hours



Click and hold down on the time cells, and drag the mouse to include the time span of your preferrence. The minimum selectable unit is half an hour. You can select separate and multiple time spans on the template.

Enter a name for the template, and click Add to save your template.

The same configuration window apply to both the Schedule template and the customize schedule windows.

If the **Events only** option is selected for the new template, you can determine what kinds of events will trigger the recording. Use the pull-down menu to select Events only.

			Add a sc	hedule tem	plate		×
Templa	te name	Schedule					
no•nn	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00:00 01:00 00:00 00:00 00:00 00:00 00:00 00:00 00:00 00:00 00:00 11:00 12:00 11:00 11:00 12:00 12:00 11:00 12:00 11:00 12:000	00:00~21:	30					
05:00	Events Only	у 🔺					
18:00 19:00	Continuo	us					
11:00 12:00	Events Or	nly					
13:00 14:00 15:00							
17:00 18:00 19:00							
20:00 21:00 22:00							
23:00 24:00							
							Cancel

When Events only is select, click on the 🍄 Settings button to proceed.

			Add a scł	nedule tem	plate		×
Templat	te name	Schedule					
00.00	Sun	Mon	Tue	Wed	Thu	Fri	Sat
00:00 01:00 02:00 03:00 05:00 05:00 07:00 09:00 10:00 12:00 14:00 15:000	00:00~21: Events Onl						
23:00 24:00							Cancel

The applicable event types will be listed. Select the types of event triggers that you prefer. Click **Apply** to leave this page. By deault, all applicable event triggers will be selected.

Select trigger events		×
_		
Motion		
PIR		
✓ Tampering		
🕑 РРТZ		
Line crossing detection		
Intrusion detection		
Loitering detection		
Face detection		
Missing object detection		
Unattended object detection		
Crowd detection		
Digital Input		
💿 Traditional recording: 💟 Trigger state 💟 Normal state		
Recording from DI activated to DI normal		
Recording from DI normal to DI activated		
	Apply	Cancel
 Crowd detection Digital Input Traditional recording: Trigger state Normal state Recording from DI activated to DI normal 	Apply	Cancel

Back on the Recording options page, select the new template as a scheduling option. Use the menu on the top to select a scheduling template for all cameras.

💙 VAST2 💿 🅸 +		cpu 7% мем 37%	III 🌲 🏟 – 😐	×
🔊 Settings	Recording options	5		
VMS_Station	G:\\Recordings			4
Recording options	3 cameras Select cameras	I	Event only Continuous None	
Failover	All cameras	Streaming	Default Schedule template-1 tempate-2	
1	FE9391-EV 192.	168.5.112 1 💌	tempate-2	
Local DB	FD8177-HT 192.	168.5.120 1 👻	tempate-2 💌	
	IP9191-HT 192.	168.5.122 1 💌	tempate-2 💌	
			Apply Cancel	

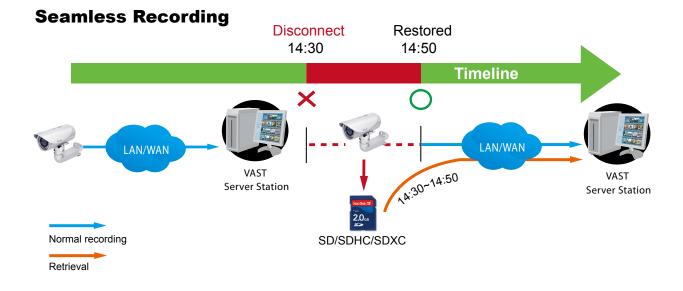
Make sure a Schedule mode is selected when you leave this configuration step.

									₩
Settings	l		Re	ecording mar	lagement				
ording options	VMS_Station	Arch	ive name 🛛		Site ₩				
ackup	Belautoroup	Stora	age + New st	orage					Recycle Options
Cocal DB		G:\\Re	cordings						
			neras Selec	I cameras	Streaming	Schedule		Seamless recording	Activity Adaptive Stream
			All cameras		1		•		
		0	FD8377-HTV	192.168.42.246	1 -	Continuous	*		

Seamless Recording

Seamless Recording safeguards critical videos in the occurences of network disconnection.

In the event of temporary disconnection, video is stored in individual cameras' SD/SDHC/ SDXC card; and once the connection is restored, a VAST server can automatically resume the recording. More remarkable is that, a VAST server can simultaneously retrieve the time-tagged videos that were temporarily stored on SD/SDHC/SDXC cards. For information about the latest firmware/software revisions that support this feature, please contact your sales representatives or technical support.



The video data retrieved from SD/SDHC/SDXC card also include event-triggered recordings such as pre- or post-event footages, if events were detected during the network outage.

The Seamless Recording feature is enabled when inserting, updating, or batch inserting cameras in the Camera Management window. The firmware/hardware compatibility of this feature is automatically detected, i.e., this feature is not available when a non-compliant camera is attached. If a compatible camera is attached, a checkbox will be available as shown below.

Raker Taker B Level 58 8 cameras B cameras B cameras	n Settings								
	ecording options	VMS_Station	Archive name Def						
Falser Luce DB S Cameras S Cameras Manne IP Streaming Schedule A downse 			Storage + New stor	nge					Recycle Options
Lucad Di 0.008condings B cameras Straming Name P Straming Schedule Adammas - Adammas - Figures -	Failover		_						
Name IP Streaming Schedule I Seamless mouting Activity Adaptive Stream Af Lamava + <td< td=""><td>_</td><td></td><td>G.1\Recordings</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	_		G.1\Recordings						
F0115-H1 122.145.5110 1 Continuous F0115-H7A 122.145.5112 1 Continuous					Streaming	Schedule		Seamless recording	Activity Adaptive Stream
1/02/165/HT-A 1/02.168.5.112 1 • Continuous •			All cameras				*		
			FE9181-H	192.168.5.110	1 *	Continuous	×		
MA3991-6TV 1 192168.5.129 1 • Continuous •			FD9165-HT-A	192.168.5.112	1 *	Continuous	*		
			MA8391-ETV 1	192.168.5.129	1 *	Continuous	*		

Activity Adaptive Stream

Activity Adaptive Stream: (Note that this feature may not be available for some older models)

This option will activate the frame rate control according to alarm trigger.

The frame control means that when there is a triggered alarm, the frame rate will raise up to the value you've configured on the Video quality page.

If you enable adaptive recording on a camera, only when an event is triggered on a camera will the server record the full frame rate streaming data; otherwise, it will only request the I frame data during normal monitoring, thus effectively saves bandwidth and storage space.

The alarm trigger includes: motion detection and DI detection. Please refer to Alarm Settings on page 145.

On individual cameras, you can configure the following:

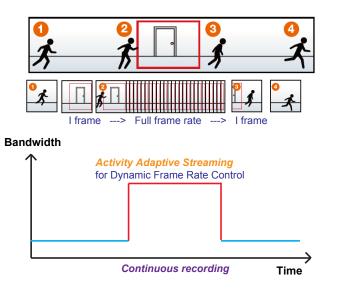
Pre-event recording and post-event recording

The Network Camera has a buffer that temporarily holds data for a period of time. Therefore, when an event occurs, the camera can restrieve image frames taken several seconds ago. Enter a number to define the duration of recording before and after a trigger is activated.

- Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.
- Source: Select a video stream as the recording source.

NOTE:

- * To enable adaptive recording, please make sure you have configured the trigger sources such as Motion Detection, DI input, or Manual trigger.
- * When there is no alarm trigger:
 - JPEG mode: record 1 frame per second.
 - H.264 mode: record the I frame only.
- * When the I frame period is > 1 second on the Video settings page, firmware will force decrease the I frame period to 1 second when the Activity Adaptive Recording feature is enabled.



Adding NAS (Network Attached Storage) as a Storage Option

You can also record videos to a networked storage.

- 1. Click the Add archive button.
- 2. Enter a name for the configuration.
- 3. Click the Add storage + New storage button.

	Recording management	
VMS_Station	Archive name Site VMS_Station O bytes available of 0 bytes	
DefaultGroup NAS	Storage + New storage	Recycle Options
	0 cameras Select cameras	

4. Click the + New NAS button.

Server	NAS	,	×
Select from	+ New NAS		

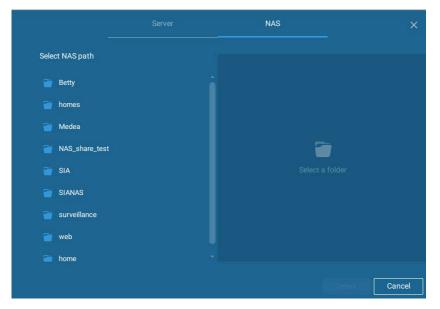
5. Enter the NAS storage's address and the credentials for access to the networked storage. When done, click the **Connect** button.

	NAS	×
New NAS storag	je	
192.168.4.162	2	
Host		
admin		
	0	Connect Cancel

6. The NAS storage should appear on screen. The connection may take several seconds. Single-click on the NAS storage to select its network shares.

	NAS	×
Select from 192.168.4.162 Host	+ New NAS	
	Edit Delete	

7. The NAS storage's network shares should be listed. Single-click to select a network share.



8. Click **Select** when done. Note that you can repeat the previous process to select multiple network shares from a single NAS storage.

	Server	NAS	×
Select NAS path			
 NAS_share_test 		\\192.168.4.162\NAS_share_test	
#recyclenew folder0002D174E769		3.27 TB available of 3.58 TB	
		Restore recordings from this path	Cancel

9. The selected shares should be listed. Enter a name and select cameras. When done, click the Add button at the lower right to complete your configuration.

	Recording management
 VMS_Station DefaultGroup 	Archive name 2.91 TB available of 3.58 TB 2.91 TB available of 3.58 TB Storage New storage V192.168.4.162 V192.168.4.162 V192.168.4.162 VAS_share_test O cameras Select cameras

2-2-3. Storage

By default, VAST will check if the D: drive is available. If no other disk drives can be specified, the system drive C: will still be defined as a storage option. Other disk drives in the system, and the default storage volume (configured in the initial setup) will be listed.

You can add a NAS storage's share volume as the additional storage option. Enter the necessary information for access to a network share. Enter and select a NAS path. The share will then be available for video recording.

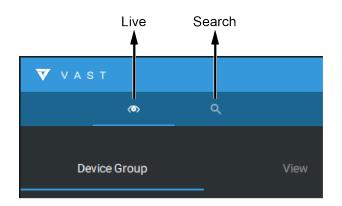
	×
New NAS storage	Select NAS path
192.168.6.117	False_NAS
Host	Users
User name	
Password	
Connect Cancel	Cancel

Select storage volumes each by a single click.

Click **Ready to use** to continue. The server will take several minutes synchronizing configuration between server and cameras, and time settings between them.

2-2-4. Starting Up - Main Page

You will be defaulted to the Live view once the main page displays. Another tab window is the Search panel where you can search recorded events and recorded videos.



On the initial start up, the server should fill the live camera feed to the available 2x2 view cells (4). You should then select a preferred layout, e.g., 3x3 or others, using the Layout pull-down menu.

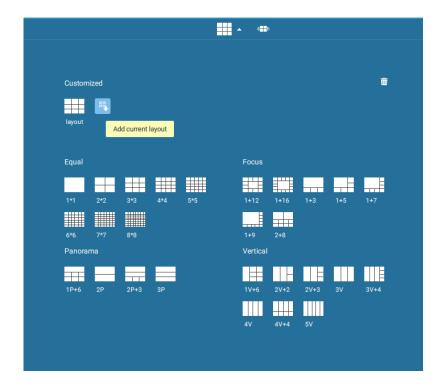
The available layouts are categorized into 4 types: Equal, Panorama, Focus, and Vertical.

Equal: 1x1, 2x2, 3x3, 4x4, 5x5, 6x6, 7x7, 8x8.

Panorama: 1P(Panoramic)+6, 2P, 2P+3, 3P. (applies to fisheye cameras)

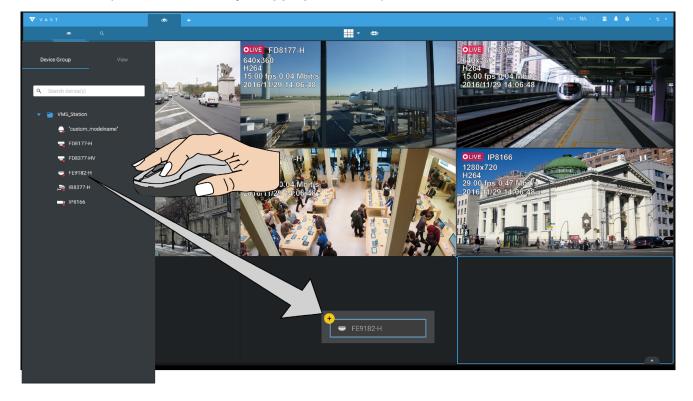
Focus: 1+12, 1+16, 1+3, 1+5, 1+7, 1+9, 2+8.

Vertical: 1V+6, 2V+2, 2V+3, 3V, 3V+4, 4V, 4V+4, 5V. (applies to corridor view)



To design and customize a layout, please refer to the Customizable Layout page.

You can then fill in the view cells by dragging and dropping cameras into the view cells. While dragging, a name tag displays. All cameras should be listed under the VMS_Station Device Group.



You can swap two view cells by dragging one on top of another.

You can also fill in an Emap by dragging and dropping a pre-configured Emap into a specific view cell. Click on the E-Map tab to select a pre-configured E-Map. Note that an E-Map should be placed into a larger view cell.

Depending on the resolution of your monitor, a view cell can be too small for an E-Map. For example, for an HD monitor (1920x1080), a single view cell from a 3x3 layout will have a resolution of 640x360. View cells larger than 330 (width) x 300 (height) pixels can contain an E-Map.



2-2-5. Saving a View

When done with arranging view cells, click the View tag.

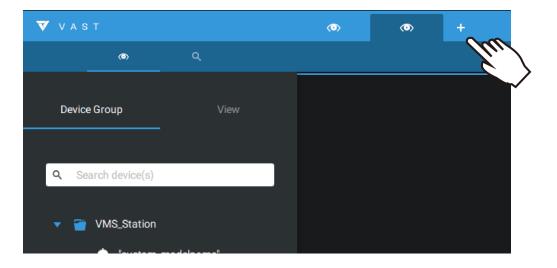
Save your current layout and view cell arrangement as a new view.

Device Group	View			×
(+		Add current view as a new View	v view	
Add as a n	new view		Add	Cancel

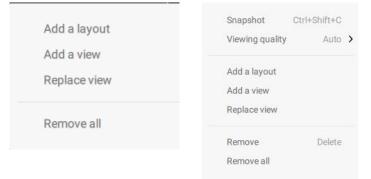
2-2-6. Add More Live Views

With many cameras in your deployments, you can click the New Tab "+" button to add more Live views.

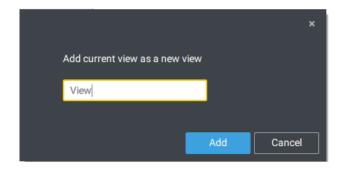
An empty live view will display, and you should repeat the above process to select a layout, and fill in the view cells. When done, save the view.



Right-click on the screen to display the right-click menu. Select Add a view.



Enter a name for the new view and click **Add** to proceed. The new view will be listed in the View panel.



If you have multiple monitors attached to your server station, you can drag a live tab to a different screen. In this way, you can display live views simultaneously on multiple screens.

Live views can be placed on up to 8 monitors. Please note that this is determined by the capability of your graphics card chipset.

▼ V A S T (®)	New tab		
Device Group View	New alarm tab Send to screen	>	creen 1
Search devices	Close	S	sreen 2
 Search devices VMS_Station VMS_Station 			

2-2-7. Save Your Preferences

Go to **Settings** \Rightarrow **Preferences** to save your current layout and display configurations.

Select the options in the startup choices menu to decide what to display whenever your VAST2 client starts. You can display Live view, Tour, Dashboard, E-Map, or Alarm tab simultaneously on multiple screens.

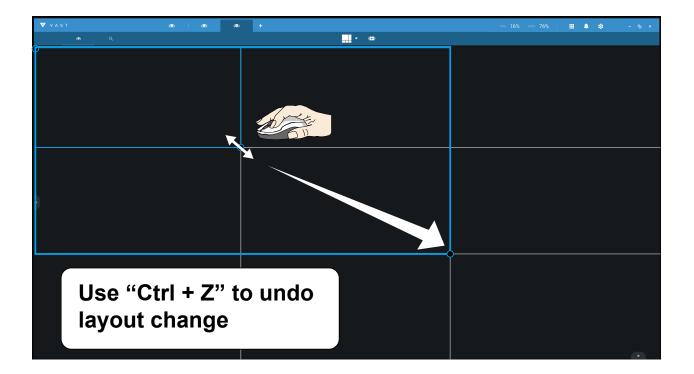
VAST2	on 🕸 +	CPU 14% MEM 28%	■
🤹 Settings		System management	
CLICINSE SMTP Preferences Feedback and bugs	Client Station	Language Peper Export Sequence format Progre Pro Progre Pro Progre Pro Progre Pro Progre Pro Progre Pro Progre Pro Progre Pro Progre Pro Progre Pro Pro Pro Pro Pro Pro Pro Pro	

2-2-8. Customizable Layout

The standard layouts can be manually configured to form layouts of your choice. Depending on the complexity of your design, you should start with a multi-cell layout.

Click and drag the corner mark on a view cell. Drag across the screen and release the mouse button to enlarge the view cell. Choose a standard layout of many view cells, e.g., 7x7 or 8x8, if you want to design a complex customized layout. You can create a special layout, e.g., an especially wide view cell for a multi-sensor camera, such as the panoramic MS-8392.

To abandon a customized layout, simply select a new layout from the layout window. You can also use the Ctrl + Z keys to undo your changes on the layout.



To preserve your customized layout, click to open the layout window. Click on the Add current

layout 🕏 button. You may then change the name of your layout by a double-click on its name. To remove a configured layout, drag it to the garbage can icon on the upper right.

• •	• +									
						•				
	Last modified		Custom	ized						Ŵ
				Ē						
			layout	layout	layout	layout				
	Equal					Focus				
	Equal					Focus				
	1*1 2*2	3*3	4*4	5*5		1+12	1+16	1+3	1+5	1+7
	6*6 7*7 Panorama	8*8				1+9 Vertical	2+8			
	1P+6 2P	2P+3	3P			1V+6	2V+2	2V+3	3V	3V+4
						4V	4V+4	5∨		
						4v	4v+4	24		
Snapshot	Ctrl+Shift+C									
Viewing quality	Auto	>								
Add a layout										
Add a view										
Replace view										
12										
Remove	Delete									

You can also right-click on the screen to display the Add layout option.

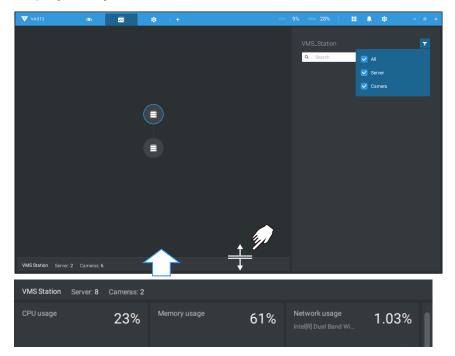
You can then click Device Group, and start filling your customized layout with camera views. When done, click **Add a view**.

Also remember to save the current layout as a view, and save your configuration in **Settings** > **Preferences**.

2-2-9. Dashboard

Select to open the Dashboard utility from the tool bar. The Dashboard displays the system resources of a CMS server along with those of its sub-stations. This provides a glimpse of the load on machines when performing the recording and monitoring tasks.

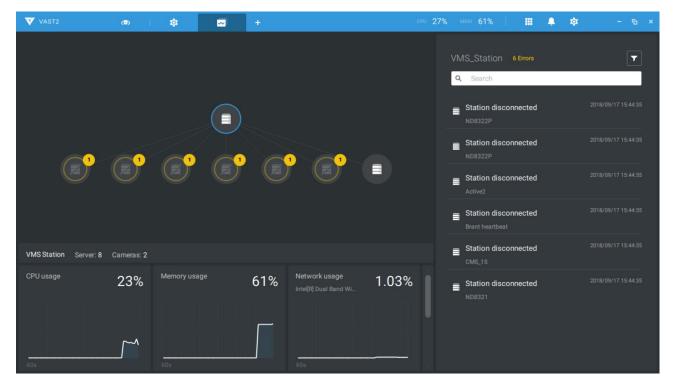
Mouse over the edge of the bottom row to reveal the expansion mark. Pull the status row up to display the system resource statuses.



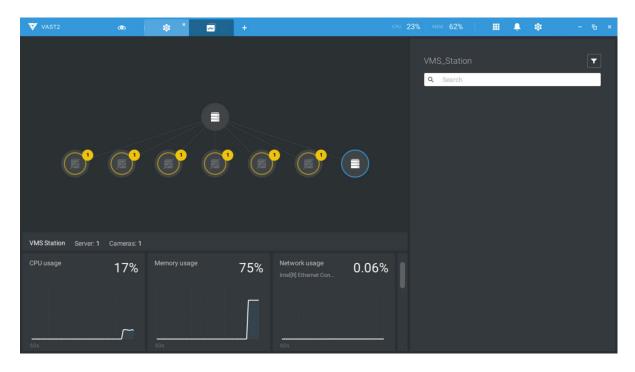
If you have multiple LAN cards or virtual HBAs, the status row can be pulled to reveal all of their statuses.

VMS Station Server:	: 2 Cameras: 6		-		
CPU usage	15%	Memory usage	29%	Network usage	0.44%
 60s		60s		60s	na na ana ana ana ana ana ana ana ana a
Network usage Intel[R] Gigabit CT D	0.00%	Network usage Isatap vivotek tw	0.00%	Network usage isatap {5453516D-2	0.00%
Network usage	0.00%				

If you have multiple sub-stations, single-click to select and reveal their individual status, including CPU usage, memory usage, and network usage.



Note that VAST servers of the earlier revisions and NVRs running older firmware do not deliver their statuses to your Dashboard.



2-2-10. E-Map

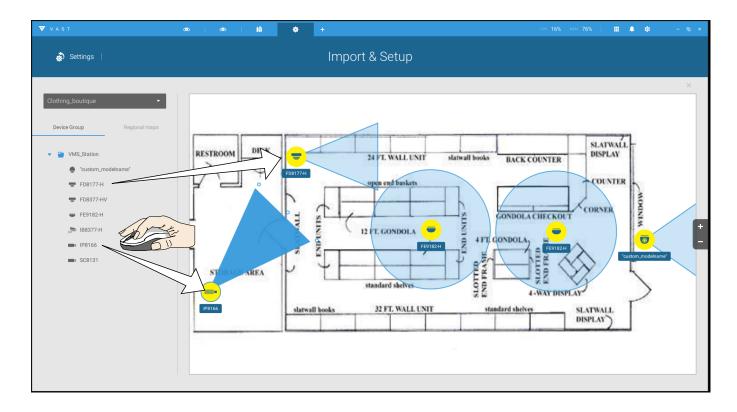
To create your E-Map, click **Settings** 🔅 . Click **Import & Setup**. Click E-Map.



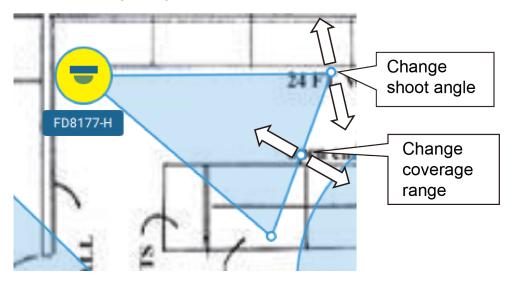
Click Import file up or Import folder . An entire folder can be imported.

When done, double-click on the snaphot of E-Map image to configure the E-Map.

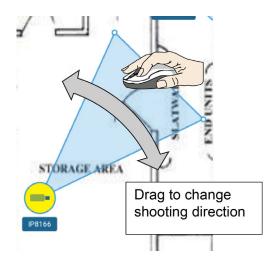
Your cameras will be listed on the left. Drag and drop the cameras to the corresponding locations on the map.



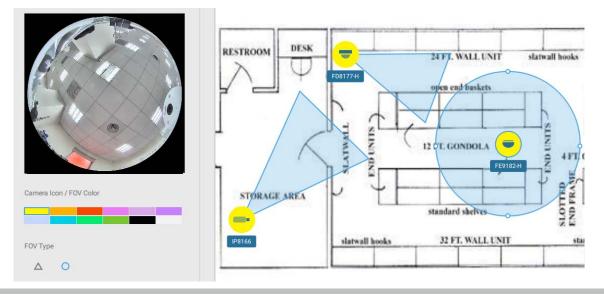
When the camera is in place, drag the FOV indicators on the edge to change the shooting angle and the coverage range.



Drag the FOV to change the shooting direction to match the actual installation.

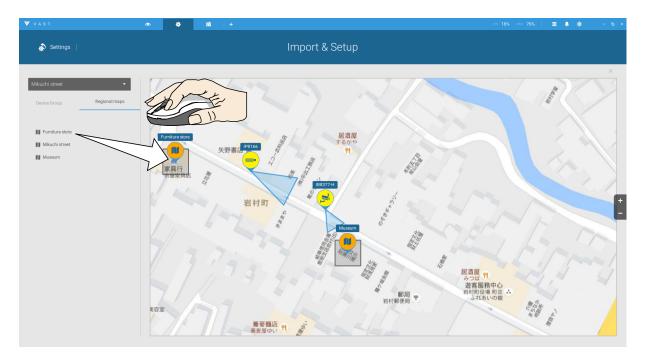


Click on the camera icon. You can also change the color of camera icon and the FOV type. Fisheye cameras, when ceiling mounted, have a round shape coverage.



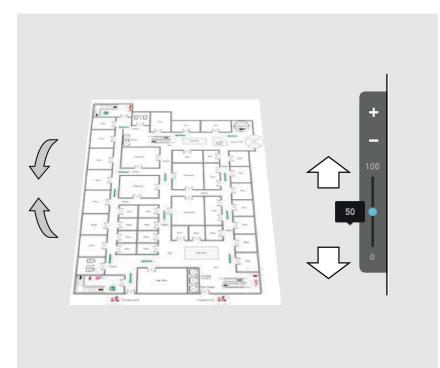
124 - User's Manual

If you have a larger regional map that covers a geographical area, say, a street block, you can drag one or many E-Maps into it. For example, you can place another E-Map that is used to indicate the camera deployment inside a building that is located on the street.



To see live streams from cameras, click on the camera icons in the E-Map.

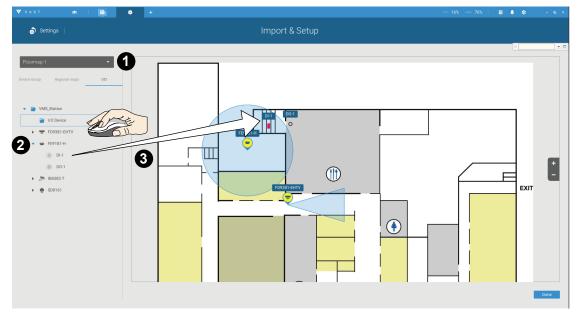
When configuring an E-Map, you can use the tilt bar on the right to tilt the E-Map image. Doing so creates a sense of distance and depth of view.



Placing DI/DO Devices

I/O devices can also be planted into an Emap, such as alarm or various kinds of detectors. TheI/O boxes (such as Advantech's Adam series) or the DI/DO connections on an NVR also apply.Select a floor map from the pull-down menu.

2. Unfold the sub-trees beneath the network camera, (taking camera DI/DO devices as an example).



3. Select a DI/DO device. Click and drag to a preferred location on map.

- 4. When a DI/DO device is selected, you can select the display colors of its icons. Configure different colors for the device status when it is normal or triggered.
- 5. When done with placing all DI/DO devices, click the Done button on the lower right of the configuration screen.



Configuring Google Map and GPS

Since Google Map changed its access policy, using the Google Maps feature requires user entering a billing API key. Using Maps, Routes, and Places APIs requires an API key.

For applying a Google API key, https://cloud.google.com/maps-platform/maps/

VAST2			N	¢	+	CPU 12% MEM 36% 🎬 🐥 🂠 - 1	o x
¢.	Settings					Import & Setup	
Google Device Group	e map Regional maps	DI/DO	GPS			6	3
•	VMS_Station FD8177-HT FE9391-EV IP9191-HT					Google Map is not available Invalid Google Map API key. Set up the Google Map API key	
						Done	

Visit Settings > Emap > All Maps.

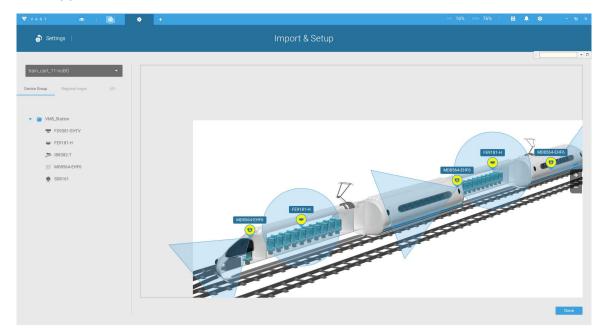
Enter the Google API key you previously registered (if using Google Map).

Google Map Settings	×
Google Map API Key	
<u>Get a GoogleMap API key</u>	
	Cancel

NOTE: In this revision, Google Map only supports installation on a GPS-enabled vehicles. Placing cameras on a static location on Google Map is currently not supported.

Before configuration on a Google Map, you should prepare an E-map drawing for special installations, such as that on a vehicle. The vehicle, e.g., a train, should come with a GPS-GSM/ GPRS module to collect the position information and passes this information to a web-server. As new data is constantly inserted to the database, the VAST server will update the location information containing coordinates, speed, distance, time, etc.; and when video recording is required, the location information and time tags will be available.

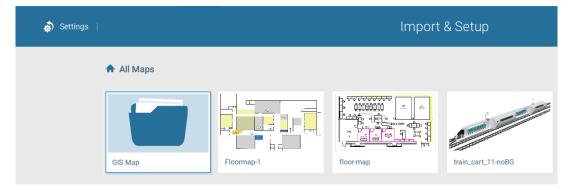
This applies to a mobile NVR that comes with GPS.



Open the E-Map Import & Setup window.



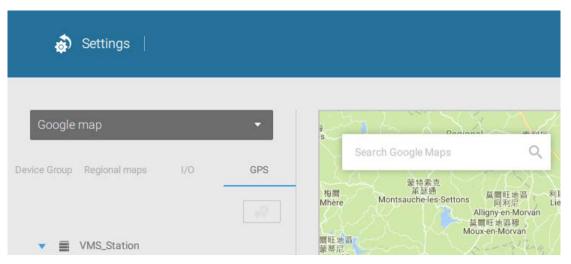
Click to enter the GIS (Geographic Information System) Map and then Google Map window.



Click on either the Google map or the OpenStreetMap.

VAST2	۲	\$	+
🔊 Settings			
	*)	All Map	os > GIS Map
	K	G	No
	Google	e map	OpenStreetMap

Click on the GPS tab. Select a VMS station or mobile NVR to apply the configuration, and then select the GPS Add button .

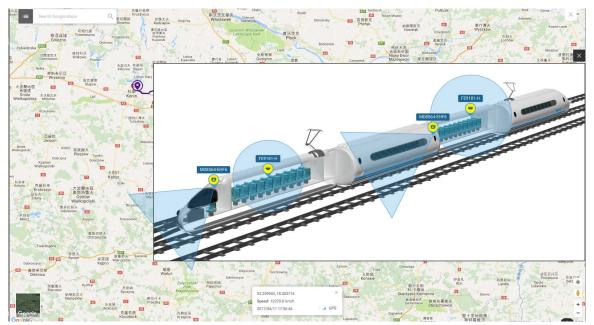


Enter a name for the GPS/GNSS server on the vehicle, its IP address, and server port number. You can select an E-map that will display when you click on the GPS location icon. Select the checkbox and an E-Map that corresponds to the deployment on the vehicle. When done, click the Apply button.

VMS_Station Self- orient 页词	
GPS Career Caree	Google Ma Re Enix Enix Bant-Nazaire

You can skip this setting for the mobile NVR that comes with a built-in GPS module.

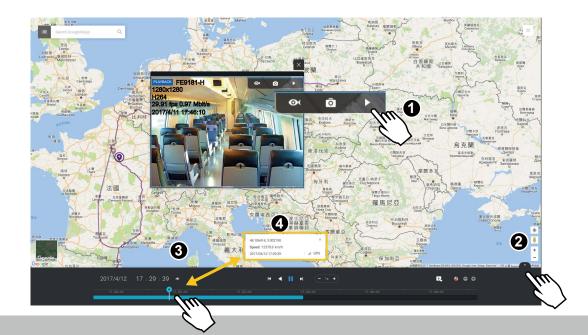
You can click on the location icon 💡 to bring up the E-Map. The coordinates, speed, and time information also display on the map.



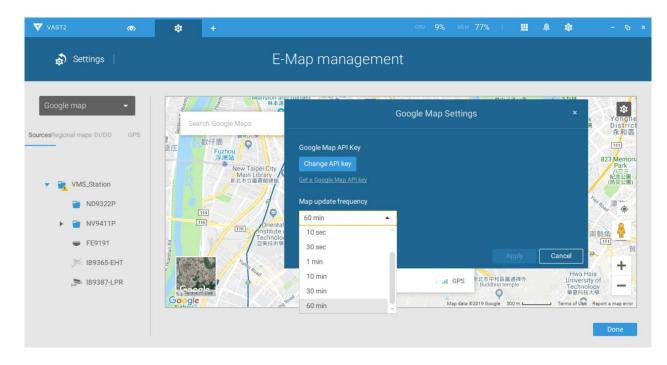
You can click on any cameras on the E-map to search through past recordings. One click displays the live view. A live stream window will display.

To search and review recordings when an event occurs,

- 1. Click on the Playback button.
- 2. Click the Pane button to display the Playback control panel.
- 3. To search for the video of past events, pull the Playhead to a point in time on the timeline.
- 4. The GPS coordinates and time will change to those corresponding to the time you selected. You can then acquire the corresponding location information while tracing the occurrence of an event.

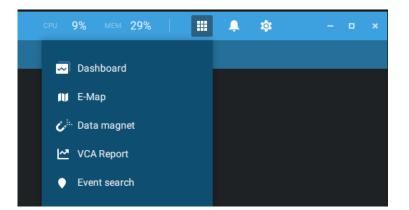


Click on the Setting button on the map to bring up the Map update frequency option. Your GPS target may travel to the outside of the map through time without the map being updated. The map will update by the interval you configure here.



2-2-11. Event Search

The Event Search window is accessed from the top tool bar.

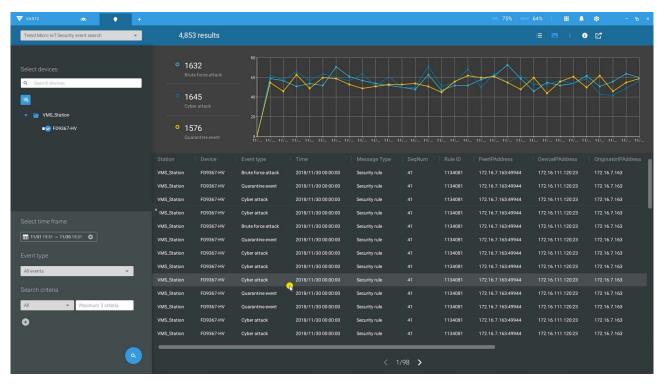


Below is the comparison between the Alarm list and the Event search windows:

Alarm List	Event Search
Reports alarms triggered by user- configurable events, such as DI/DOs, Motion Detection, tampering, VCA analytics, cybersecurity, and so on.	The events on the Event Search window require no user configurations. The Event Search window displays system events and provides a glimpse of all general events.
	The event types include: General events, Smart VCA events, and Trend Micro IoT Security events.

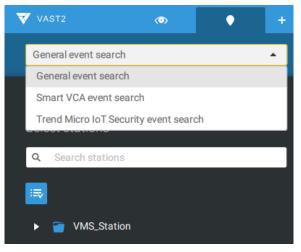
The sample screen for VCA-related events is shown below:

💎 VAST2 🔷 🕇				CPU 7%	MEM 79% 🏭	🌲 💠 – 🕫 ×
Smart VCA event search	*	1,1	80 results		·= 🖬	· ۲
	_			Event type		Description
Select devices		VMS_Station	10.17.2.49	Intrusion detection	2019/06/25 10:04:26	Rule name=Intrusion, Type
Q. Search devices		VMS_Station	10.17.2.49	Intrusion detection	2019/06/25 10:04:16	Rule name=Intrusion, Type
=		VMS_Station	10.17.2.49	Loitering detection	2019/06/25 10:04:12	Rule name=Loitering
VMS_Station		VMS_Station	10.17.2.49	Intrusion detection	2019/06/25 10:03:04	Rule name=Intrusion, Type
		VMS_Station	10.17.2.49	Loitering detection	2019/06/25 10:02:53	Rule name=Loitering
		VMS_Station	10.17.2.49	Intrusion detection	2019/06/25 10:02:49	Rule name=Intrusion, Type
Select time frame		VMS_Station	10.17.2.49	Intrusion detection	2019/06/25 10:02:16	Rule name=Intrusion, Type
		VMS_Station	10.17.2.49	Intrusion detection	2019/06/25 10:00:19	Rule name=Intrusion, Type
		VMS_Station	10.17.2.49	Intrusion detection	2019/06/25 09:59:21	Rule name=Intrusion, Type
Event type		VMS_Station	10.17.2.49	Loitering detection	2019/06/25 09:59:17	Rule name=Loitering
All events 👻 👻		VMS_Station	10.17.2.49	Loitering detection	2019/06/25 09:59:08	Rule name=Loitering
				< 1/24	>	

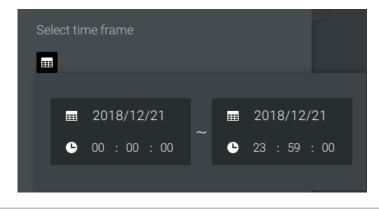


The sample screen for network security-related events is shown below:

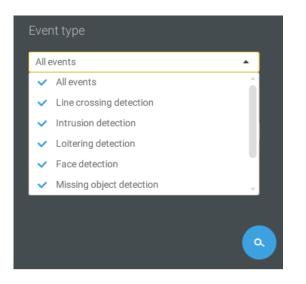
From the Search Event window, you can view and search events by its event types, and use the Export button to save a record of these events (in the CSV format).



Use the calendar tool to specify the span of time as the search range.



Use the Event type menu to narrow down the types of events. Select or deselect the event types for search. You may also enter one or several keywords as the search criteria in the following menus.



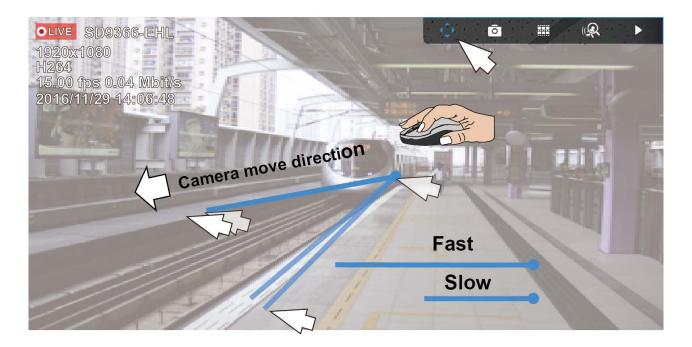
Click the search button to generate search results.

2-2-12. PTZ Control

PTZ on this page refers to the mechanical PTZ. The discussion on this page applies to cameras that come with PTZ mechanisms that are capable of directional and zoom control.

To begin the PTZ control, click on the PTZ 💽 button.

Click and drag your left mouse button across the screen, towards the direction you wish to move. A light blue trace will appear. The longer the trace, the faster the move.



Note that while the camera is moving, you can change the move direction keeping the mouse button hold down. Release the button to stop moving.

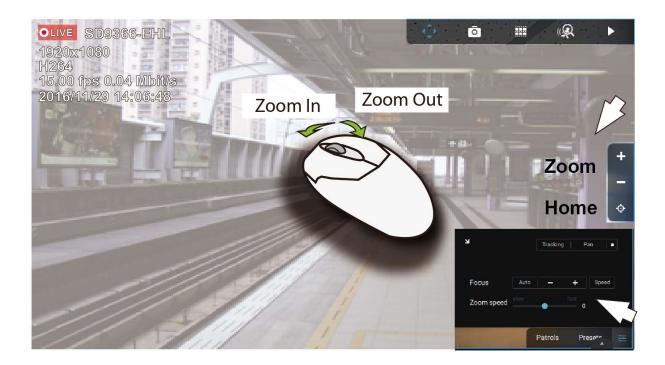
See Appendix C Joystick support if you use VIVOTEK's joystick.

You can also use the mouse wheel to zoom in or zoom out. You can also mouse over the right side of the screen to display the zoom button. A home button is also provided.

The Patrol, Presets, and PTZ control panel is located at the lower right of the screen. You can click to begin a pre-configured patrol, preset points, or enable a Tracking or Pan action.

You can also adjust the Zoom speed, and/or manually adjust the Focus and the Focus speed.

See Appendix F Smart Tracking for how to enable the Smart Tracking feature.



2-2-13. Playback

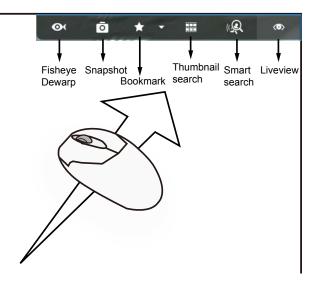
To start the playback function, select a camera's view cell (whether in full view or ordinary cell

size), then click the playback initiative button (). The button can be found on the upper right of the view cell or at the lower right corner of the view cell in the full view.

Default Time: When started, system normally rolls back to the start of the hour, e.g., your current time is 10:30:00, and the default playback position on the timeline is 10:00:00.

Playback control can be found in 3 places:

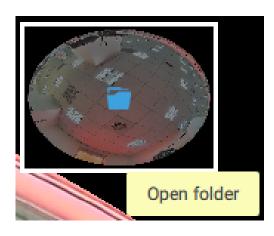
1. **Float Panel**: When Playback is started, swipe your mouse to the upper-right of the view cell to display the Playback float panel.



Fisheye Dewarp: For a fisheye camera, you can select different dewarped views during a playback. Click to select an option.

Snapshot: Click to take a snapshot. A small floating window will stay for 2 seconds. You can click the folder icon to access the snapshot files.

Note that a dewarped, regional view allows producing a snapshot of the regional view.

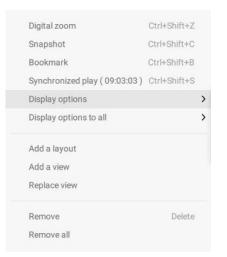


Bookmark: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos. Note that the bookmarked video clips are free from storage recycles. They will not be erased when storage space runs short and needs to be recycled.

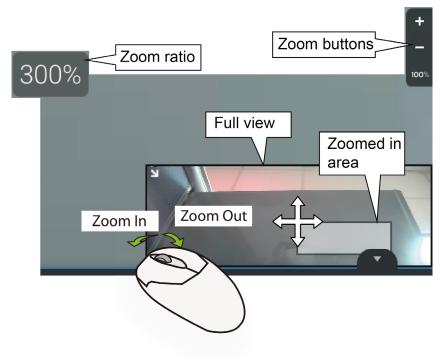
Smart search II: Smart search II is an independent function. See page 168 for details.

Liveview: Click to return to Live view.

2. Right-click Menu: Right-click on the Playback screen to display this menu.



Digital zoom: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos.



Snapshot: Click to take a snapshot. A small floating window will stay for 2 seconds. You can click the folder icon to access the snapshot files.

Bookmark: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos.

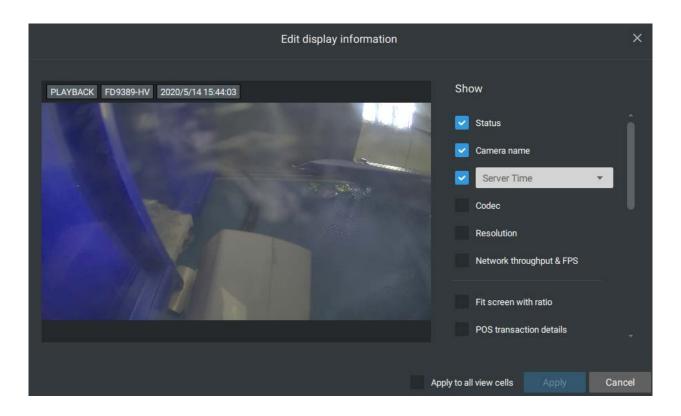
Synchronized play: When enabled, all cameras in the same view will be playing the video of the same point in time.

The following commands are general purpose commands.

Display information: By default, all display elements will appear on screen for all playback windows. You can use the Edit display information to select more display elements.

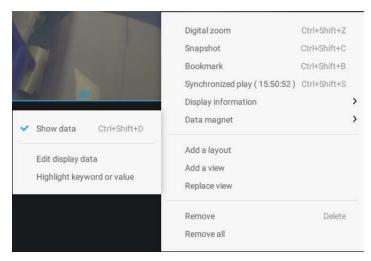
They include:

Status, Camera name, Server time, Codec, Resolution, Network throughput & FPS, Fit screen with ratio, POS transaction details (for POS), Data magnet data (Data overlay on screen / Hide data after idle), Motion detection, Rules (VCA), Rule name, Motion cells, Tracking block, Tracking dot, Exclusive area, People detection area.

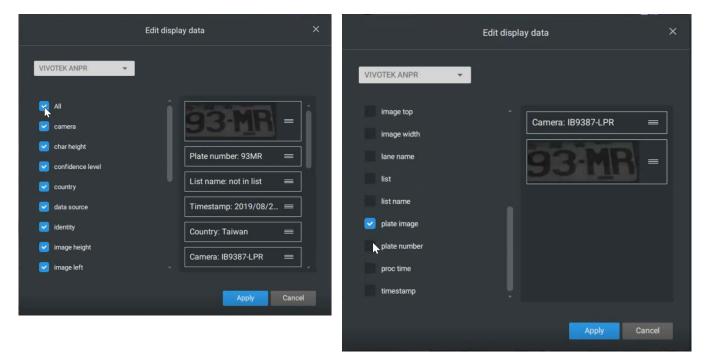


Data magnet: For 3rd-party applications, such as VIVOTEK's license plate recognition software, you can select to display different types of information. You can use the Edit display data to select or deselect the display elements.

Please note that the display elements can vary for different applications.

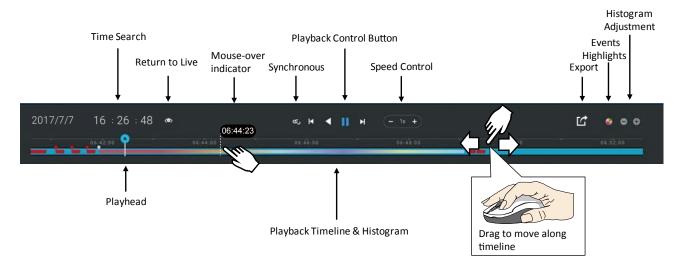


Below are the sample screens for applications implemented via the Data magnet.



3. Timeline Panel: This panel appears when Playback is initiated.

Timescale is adjustable (minutes, hours, days, to a max. of 3 days) so you can easily find the required time period and begin playback from that point.



Starting from left to right, timeline control functions will be described as follolws:

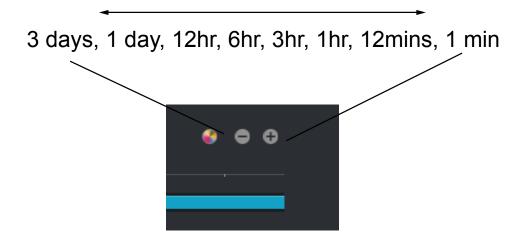
1. **Time Search**: Click on the current date to open a calendar. If you want to review videos recorded in another day, select it from the calendar.

Dec, 2016					<	>
Sun	Mon	Tue	Wed	Thu	Fri	Sat
27					2	3
4	5	б	7	8		10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1						7

Blue: days with recordings. Orange bottom line: Today. White: days with no recordings. Click on the current time. You can use the arrow buttons to change the time you wish to playback, or simply enter a preferred number. You can also pull the playhead along the timeline.



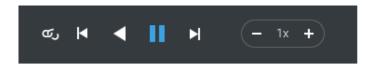
Timeline magnification levels: The default time span is 6 hours. You can change the magnification level for easier browsing. Click the Zoom in and Zoom out buttons to change the timeline time span. The configurable time spans are shown below:



2. Playback control:

From left to right,

- 2-1. **Synchronous play**: This lets all cameras in the same view to playback video of the same point in time. If you perform synchronous playback on a multi-cell view, your computer can be stressed. It is recommended you create a new view with a 2x2 layout, select and insert camera views into it, and begin the Synchronous playback.
- 2-2. **Frame by frame buttons**: Click to move forward or backward to flick through the video frames. This may only display the I-frames.



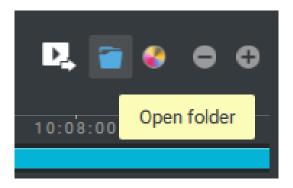
2-3. Forward playback and reverse playback: Click to view the video in the forward or reverse playback manner.

2-4. Speed selector: The selectable speed ranges from 1/64x to 64x.

3. Export Clips: Click the Export Clips button . A range selector will appear. Pull the ends to include the time span you want to export. Note that each end of the selector, when clicked and selected, will turn white, and its location on the timescale is shown on the time line. When done, click the Start to export button.

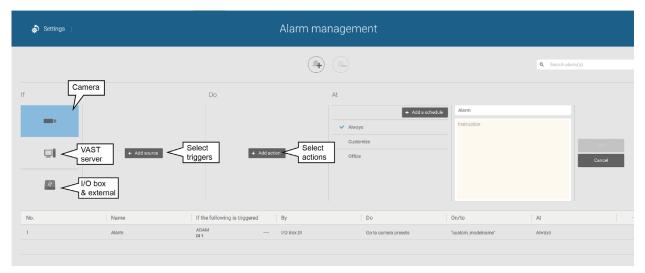


Depending on the length of video clips to export, it may take minutes to export. When the export is completed, a shortcut to the exported clips is shown. You may then open the folder where the clips are located.



2-2-14. Alarm

The Alarms can be configured to perform a series of actions when different events occur. Alarms can be used to automatically react to possible threats. For example, the VAST server can start a recording or send an Email notification when Motion detection is triggered.



A wide variety of triggering conditions can be applied, including:

1. Camera triggers

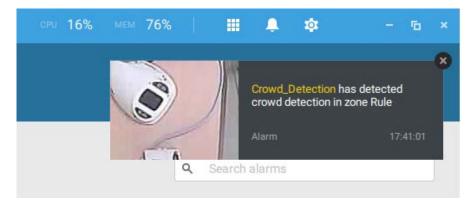
Ge	eneral		
•	Motion detection	•	IR (Infrared)
	Camera DI	•	PIR (Passive Infrared)
•	Camera DO	•	Tampering detection
	Temperature	•	Stop recording
•	Recording error	•	Audio detection
•	Video loss (Video server only)	•	Shock detection
•	SD card life expectancy detection		
Vi	deo Content Analysis		
•	Line crossing (VCA)		Intrusion detection
•	Loitering detection		Face detection
•	Missing object detection	•	Unattended object detection
	Crowd detection		Smart tracking
•	Zone detection		
Tr	end Micro IoT Security		
•	Brute force attack	•	Cyber attack
	Quarantine event		

Note that some of the triggers require that you open a web console to individual cameras. For example, VCA and Motion detection windows have to be manually configured on each camera before they can be configured in the Alarm settings.

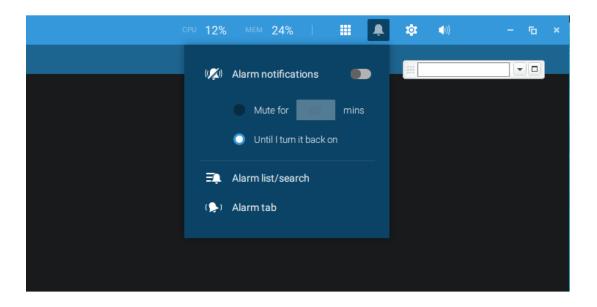


If you select a trigger and you cannot find a corresponding device, you need to open a web console to that device. Make sure the corresponding VADP is running. Open the VAST2 device tree, right-click on the device to perform a manual refresh "Update device" to acquire the lastest configuration update.

If a triggering condition is associated with event recording, an event prompt will pop up on the screen when a triggering condition is met. For example, the number of people exceeds a preset threshold in a Crowd Detection configuration. The sample prompt is shown below. The related footage can be played back by clicking on the event entry.

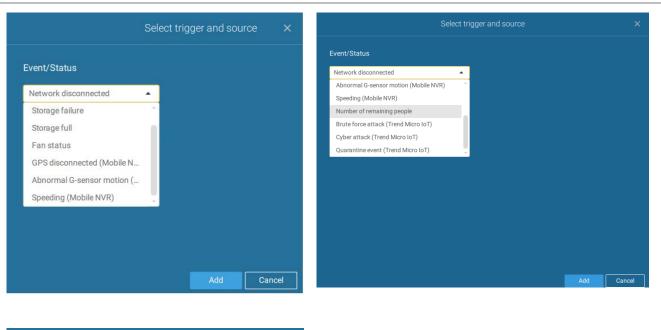


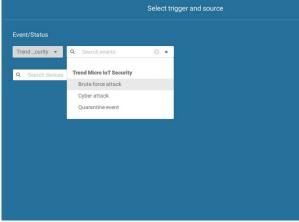
On the Alarm tab, you can select to mute all alarms for a configurable period of time. Enter the number of minutes or select to mute until you manually turn it back on.



2. VAST server and NVR trigg	gers 🛄
 Network disconnected 	These can be used to send maintenance notifications.
Storage failure	
Storage full	
• Fan status	
GPS disconnected	The GPS and G-sensor related options apply to the Mobile
(Mobile NVR)	NVR that comes with the GPS and G-sensor. GPS can be
 Abnormal G-sensor 	used to track the speed and location of a vehicle, while the
motion (Mobile NVR)	G-sensor can be used to detect abnormal impact.
Speeding (Mobile NVR)	
 Number of remaining people 	For VCA-capable cameras, the alarm can be triggered when the number of people staying within a specific area has exceeded the preset threshold. For example, when too many people are waiting in line in front of a cashier.
	This function requires appropriate configuration on the counting camera(s).
Brute force attack (Tren	d These can be configured as alarm triggers to notify the
Micro IoT)	administrator that malicious attacks have occurred. Note
Cyber attack (Trend Micro	^D that these triggers are available with NVRs that come with
loT)	the protection of Trend Micro IoT packages.
 Quarantine event (Trend Micro IoT) 	

* Note that you should use the pull-down menu to select a triggering condition, and then click to select a mobile NVR.





Note that the alarms will be received into the Alarm list window. The previous Alarm Search window is replaced by the Alarm list function.

The Alarm tab window is used to display the live video stream when an alarm is triggered, and its responding action is configured as "Send live streaming."

For I/O box configuration, please refer to the I/O Box page.

3.	I/0	box	and	TCP	triggers	-
----	-----	-----	-----	-----	----------	---

	DI/DO Device DI	This applies when an external I/O box is applied, e.g.,
•	DI/DO Device DO	Advantech's ADAM I/O box.
•	TCP Message	TCP message comes from the peer VAST servers or external sources (such as an access control system) via the analysis of received TCP message over the 3444 port. This is a paid feature.
•	Data Magnet	Triggering conditions can be acquiring data from 3rd-party software, such as the character height, image width, list, list name, country, from an LPR software, etc.

To configure a TCP message trigger,

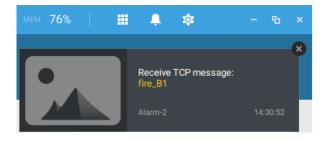
Select TCP message as a trigger type, and enter a description, such as a short term, for VAST to listen and analyze data packages.

Select trigge	er and source X
Event/Status TCP Message (Using default port 3444)	VMS_Station
Q Search devices	Trigger alarm if receive TCP message
VMS_Station	text contains 🔹
	TCP message (Maximum 128 characters)
	Case sensitive
	No repeated triggers within 5 s 1~30s
	Apply Cancel

Below are the messaging parameters:

- 1. text contains: Messages will be received if some of the textual messages match the keywords.
- 2. text matches: Textual messages must be exactly identical.
- 3. Case sensitive: The upper or lower cases letters used in the messages must match within the messages.

You can use Telnet to send a small amount of data matching the term you entered in the TCP message configuration window. A TCP message event will be triggered, and you should see the event prompt as follows.



•	Start to record video	•	Send HTTP requests
•	Set DO status	•	Send live streaming
•	Go to camera presets	•	Send email
	Go to E-map	•	Sound the alarm
	Add bookmark		

The available actions include:

The Start to record video will record a video clip of the length of 10 seconds (default) on the occurrence of an event. The event recording pre / post event time is configurable. Except for Stop recording, all the other triggering conditions can be associated with this action.

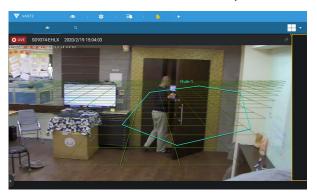
The Set DO status will activate a DO connection. For example, to light an illuminator or sound an alarm.

You can select a camera, and its DO pins will appear on the right. You can configure the duration of the DO trigger, e.g., 15 seconds.

If no Trigger period is configured and when there are multiple instances of DO trigger, administration troubles may occur. Use the arrow marks to configure a trigger period. You may also manually enter a number.

Select a	actions		×
Set D0 status ▼ Q Search devices ● ● ● VMS_Station ● ● ● FD9387-HTV-A ●	FD9387-HTV-A Select DO OD-1 V D0-2	 Trigger Normal Trigger period 5 s 	
		Add Can	cel

The Send live streaming action will bring up a video prompt to the Alarm tab window, showing the realtime video feed from a specific camera.



The Go to camera presets requires you to configure preset points on a PTZ camera before the Alarm configuration, such as a speed dome. Once triggered, the PTZ camera lens will move to a preset position.

The VAST server automatically disables unavailable options. For example, when the DO option is selected, the cameras that do not support DO connections will be hidden.

The Send email opens a configuration page where you should enter valid email addresses as sender and recipients. It is required that you configure an SMTP server for mail delivery in Settings > SMTP. Enter Subject and contents. Select the checkbox for including a snapshot of the event. When done, click Add to enable the action.

The Go to E-map opens a pre-configured E-map of where the triggering condition occurs. The user can then click on the camera icon on the E-map for an instant viewing.

The Add bookmark function saves a video clip of a 10-seconds length. Once triggered, you can open a new view tab > Search > Bookmark search to find the existing bookmarks. The bookmarked video clips will not be recycled during the storage cleaning cycles.

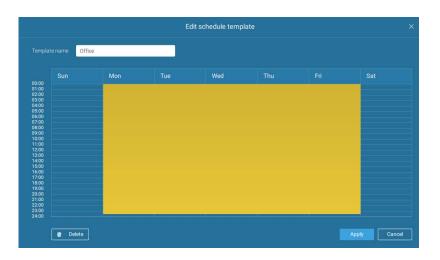
The Sound the alarm action provides 5 alarm sounds that will be sounded on the VAST client or server. Your VAST client or server should have speakers for playing the audible alarm.

	Select actions		×
Sound the alarm	•		
Select an alarm sound:			
Alarm 1			
Alarm 2			
Alarm 3			
Alarm 4			
Alarm 5			
		Add Cano	cel

A reacheable Mail server and Email accounts must be provided before you can apply the settings.

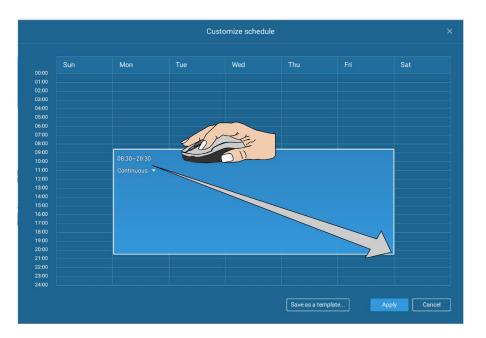
	Sel	ect actions	×
Send email			
Sender's email	test@gmail.com		
Recipient			
Subject	Alarm Notification		
Content	Device: \$(DeviceName) Trigger: \$(TriggerType) Time: \$(EventTime)	•	
		Add Cano	xel

On the **Schedule** page, you can select to activate or de-activate alarm triggers throughout a specific timeline. For example, in some situations you can disable the alarm triggers during the office hours, and choose to enable the triggers only during the off-office hours.



Click on any of the options on the Schedule panel for the alarm to take effect: Customize, Always, or Add a schedule.

You can manually create a effective time template using the New template Save as a template... button.



Click and hold down on the time cells, and drag the mouse to include the time span of your preferrence. The minimum selectable unit is half an hour. You can select multiple time spans on the template. Enter a name for the template, and click Add to save your template.

The same configuraion window apply to both the Schedule template and the customize schedule windows.

Make sure a Schedule mode is selected when you leave this configuration step.

Enter a name and instructions for users to follow, and then click Add to complete the Alarm setting.

All configured alarms will be listed on the Alarm settings page.

Group Alarm

Multiple triggered alarms can be presented as group alarms. Alarms triggered by the same event type, and by the same camera can be grouped together. In this way, multiple similar alarms can be listed under one entry.

(On the ala	arm	۱ li	st,	click	the	Group alarm	button to	disp	lay the	e ala	arm g	grou	Э.	
	VAST2				₹.	+									

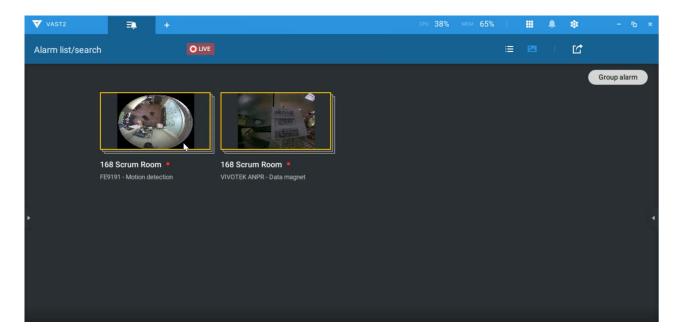
VAST2 💿	i 🌣 🗎	+				PU 15% Mi	ем 35%	1	Ļ.	\$	- 6
Alarm list/search	O LIVE							= 1		ഥ	
											Group alarm
▼ 168 Scrum Roo	om (FE9191 - Motion detec	ction) •									
										· · ·	
					Click to re	eveal the	e video	viewi	ng pa	nel.	

In the list mode, you can expand the right-hand-side panel. The video of the latest alarm will display.

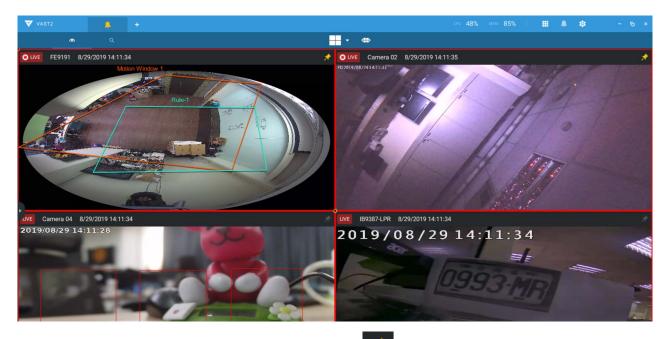
When the alarm-triggered action is configured as sounded alarm, you can mute all alarms in the group by clicking the alarm sound icon.

		Name	Station	Trigger source
	Þ	Alarm (FE9181-H - Motion detection) •		
	•	Alarm (FE9181-H - Motion detection) •		
0		Alarm	VMS_Station	FE9181-H - Windo
		Alarm	VMS_Station	FE9181-H - Windo
		Alarm	VMS_Station	FE9181-H - Windo
		Alarm	VMS_Station	FE9181-H - Windo

The same applies to the thumbnail view. To leave the group alarm view, click the Group alarm button again.



When the alarm action is set to "Send live streaming," the videos coming from the same camera will occupy only one view cell.



In the Alarm tab window, use the thumbtack *button* to freeze the current screen. If thumbtacked, the other incoming alarms will not affect the current screen.

On arrival, the latest alarm will display with a blinking red frame. A selected view cell will display with a yellow frame.

The alarm notification can be turned off by clicking on the Alarm tab. Use the slide toggle to do so. You can also select to let the notification automatically turn on after a configurable span of time. Enter the number in the mins field. The max. time span is 9,999 minutes.

The notification configuration is kept on the client computer.

When the Alarm notification is turned off, the Alarm tab icon is greyed out igaplus

VAST2	۲	÷	₽		cru 12%	MEM 37%		\$ - •
Alarm list	/search	O LIV	E		(1)	Alarm notification Mute until 15:49, 09/09	s 💿	Ľ
						Turn on in	10 mins	
				Event type		🛑 Until I turn it ba	ack on	
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 ᇘ	Alarm list/search		
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09	Alarm tab		
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09			
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:50:44	Ni		
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:50:39			
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:50:33		168 Scrum Ro VMS Station	om
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:50:28		FE9191 - Wind	ow 1
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:50:23		Status In p	progress 👻
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:50:18			History
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:49:55			
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:49:30		Updated statu	s to In progress
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:49:24		1	
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:49:19			
	168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/09/09 14:48:55			
	2019/9/2 1	3:34:05		H 4 Þ			ß	
	2019/9/2 1	0.04.00					2	

Note that the default for the alarm notification is "Until I turn it back on." If you turn off the alarm notification, you need to re-activate it after you turn off the notification the first time.



2-2-15. Search Panel

The Search panel is accessed via the Search substitution. 2 key functions are provided: Search by **POS** transaction, and Search by **Bookmark**.

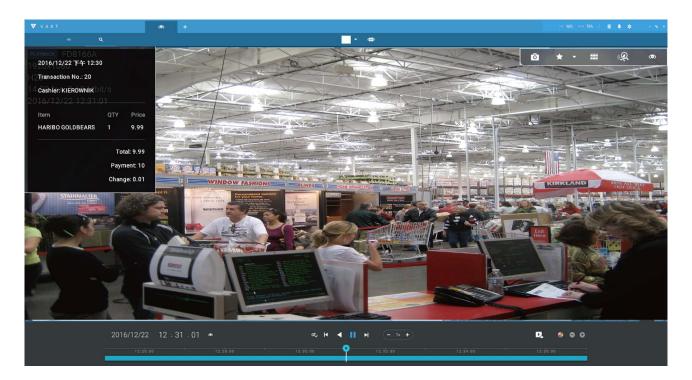
1. Search by POS transaction: The VAST station can collect coordinated database information from a POS machine. This function provides access to the video clips associated with the sales record on the POS machine. Details of transaction can be listed on screen so that a manager can see the live view when controversial events occur.

To search the POS-related recordings,

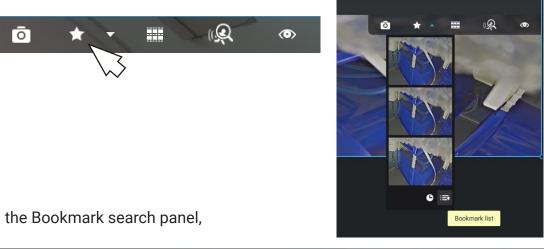
- 2-1. Select the VAST station which the POS machine is connected to (via the Settings > POS configuration).
- 2-2. If you know the approximate time of occurrence (bill void, content adjusted, shortage of products, and other frauds), use the calendar to select a time span.
- 2-3. Select a POS machine, if there are many.
- 2-4. Select a search condition, such as item name, subtotal, or the transaction number. You can use the >, <, or = signs to specify the amount you are searching for. For example, key in >100 for amounts larger than \$100.
- 2-5. You can click the add button below to append more search conditions.
- 2-6. When done, click the search button.



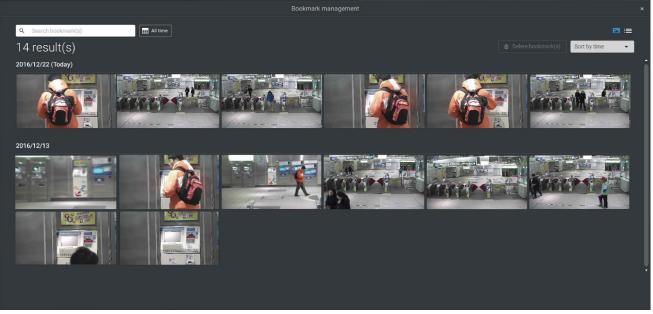
NOTE: The Alarm search panel is replaced by the Alarm list function. The Alarm list is accessed from the top tool bar. 2-7. Click on any of the search results. Details of the transaction will display along with the recording of the time of occurrence.



2. Search by Bookmark: Bookmarks are manually created when users review recorded videos in the Playback mode. Each bookmark comes as a 10-second video clip.



In the Bookmark search panel,



Click the Bookmark search 🖾 button. The Bookmark Management window will prompt. All existing bookmarks will be listed with thumbnails.

- a. On this window, you can specify a range of time during which the video streams were recorded and its points in time were bookmarked.
- b. You can then click on a bookmark to display the short video clip extracted from within the recorded video. The default is 10 seconds.
- c. To remove an existing bookmark, left-click to select an entry, and then click the Delete bookmark(s) button. Bookmarks will be indicated as "Invalid" if the videos where the bookmarks were appended were erased, e.g., when the original recording was erased by cyclic recording.
- d. Currently you can search for bookmarks using the name of the camera.
- e. You can also select the display types for the bookmark search in either the thumbnails or list mode.

2-2-16. Smart search

The Smart search function enables a quick glimpse of activities occurred within a userconfigurable detection area from the recorded videos. **Smart search** is available in both the **Liveview** and **Playback** mode.

Click to select a camera view cell. Click on the Smart search button is to enter the Smart search window.

There are two Smart Search modes: Smart search II and Smart search I. The Smart search II applies to the recordings of the cameras that come with the Smart Motion, and other VCA capabilities. There are two kinds of metadata polled from camera VCA packages:

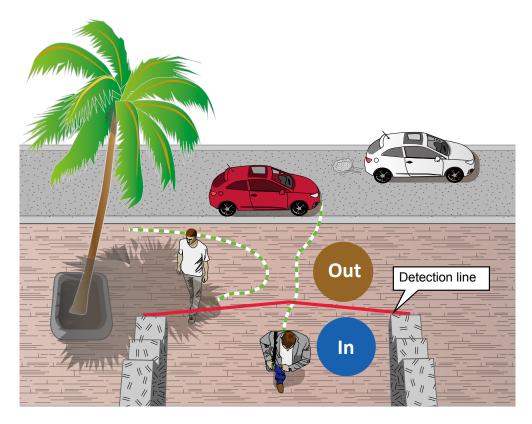
- 1. Motion cell: Pixel-based information. The search results will include all moving objects in the scene.
- 2. Object information: Human-based information. If People detection is selected, only objects detected as human will be displayed as the search results.

Please refer to VIVOTEK's website pages that are related to the Smart motion and Smart VCA features for the supported cameras.

Below are short description for the Line Crossing, Loitering, and Intrusion detection functionality:

Line Crossing Detection

The Line Crossing detection detects one or multiple persons crossing a virtual trip-wire. The traffic direction can be assigned on screen for persons passing the line in one specific direction or in both directions.

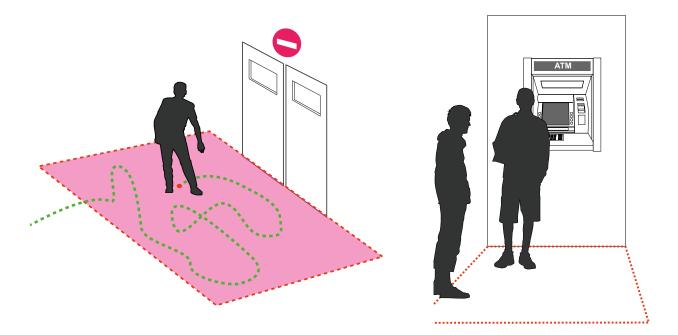


The applicable scenarios of this feature can be:

- * Detects someone who enters a drive way, entrance, or exit through the virtual line.
- * Detects and triggers an alarm in a predetermined direction.
- * The detection line can be used as a fence boundary to know if someone has crossed the articulated line around a perimeter.

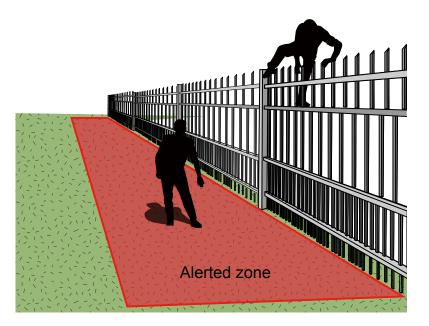
Loitering Detection

The Loitering detection can be used to detect a person or a group of people lingering in an area for longer than a preset time threshold.



Intrusion Detection

VIVOTEK Intrusion Detection can be used to detect people entering or leaving a virtual area in the camera field of view.

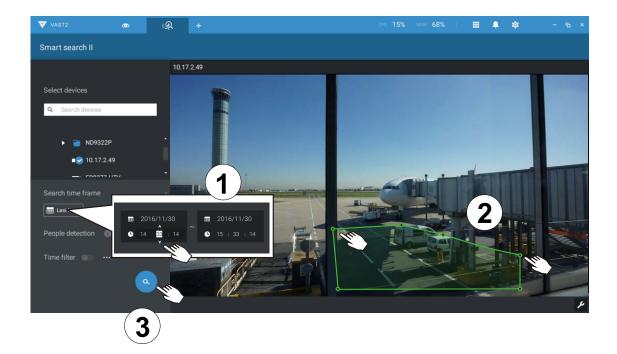


The applicable scenarios of this feature can be:

- * Detects when a person enters a bank vault or school after the office hours.
- * Detects when a person leaves an emergency exit or fire escape, or any place that is normally forbidden from access.

To use Smart search,

- 1. Use the date and time selectors to specify a time span on which to perform the Smart search.
- 2. Select a Type (Smart motion, Line crossing, Loitering, or Intrusion). Selecting Line crossing detection may require you to adjust the position of the detection line.
- 3. There are different parameters for each detection Type. Refer to each VCA feature's documentation for details. You can tune the parameters for each VCA feature. See next page for the configurable parameters.



- 4. You can draw one polygon with multiple mouse clicks to include areas where activities of your interest have occurred. You can draw one or more cross lines for Cross line detection. Double-click to close a polygon.
- 5. Click the Search button.

Search parameters:

Search time frame	Use the calendar scene will be sear Search time frame 2020/2/11 • 10 : 26 : 44	ched.	fy the time span	within which the activities in				
Туре	If the selected car supported types w Smart motion, Li	vill be listed:		detection features, the				
Parameters	Smart motion	Line crossing	Loitering	Intrusion				
(determined by Type)								
	People detection*	People walking direction	Stay time	Direction: Into the zone / Leaving the zone				
	Sensitivity**							
	Time filter							
* People detection	People detection enables the display of the alarms detected via the human silhouettes algorithm. This can be used to filter out video analytics alarms that are not related to human activities, such as swaying vegetation, or small animals.							
** Sensitivity	-	Configure the sensitivity for the detection of the activities in scene. Low for near scene, high sensitivity for long distance scenes.						

Note that different cameras support different VCA functions. Please refer to the documentation for Smart VCA or Smart tracking features, such as the **Smart VCA User Guide**.

IMPORTANT:

Running Smart Search II requires cameras that support the following:

- 1. Smart motion.
- 2. Firmware version above 0113d, 0117b or 0100i (Authwebsocket support is needed)
- 3. VCA package version above 6.1.3a.

NOTE:

- * Smart search II supports people detection whether the camera comes with a Smart motion license or not. However, the Line crossing, Loitering, Intrusion features will not be available.
- * With a valid VCA package and license, the abovementioned features will be available in the Smart search II.

In most cases, it is presumed that you have configured VCA detection zones and detection rules such as lines to detect people crossing. You can also configure a detection zone or lines on the VAST server and then search for the detection results from the recorded videos.

If your camera supports Smart VCA features, you can manually create detection rules on the configuration screen. Note that you may not need to do this if you have already configured detection rules on the camera.

- 1. Select a VCA camera.
- Select a VCA type from the pull-down list: Smart Motion, Line crossing, Loitering, or Intrusion.
 For a camera that supports only one VCA feature, such as Smart tracking on a speed dome, there is no "type" option.
- 3. You can then draw a detection zone, or detection line on the screen.
- 4. Select a time frame using the calendar tool.
- 5. Select to enable or disable the People detection feature and configure the Time filter, or other parameters.

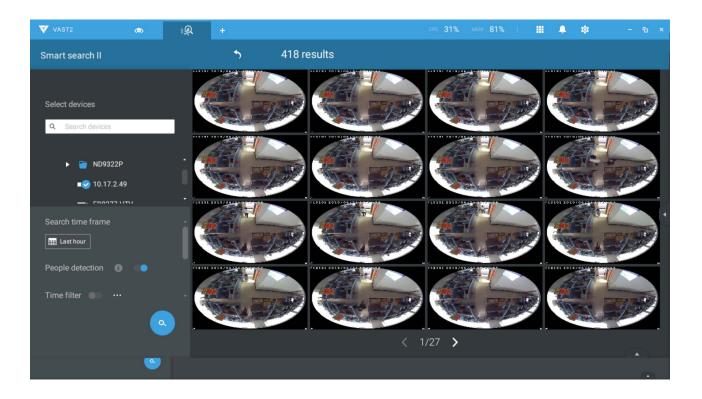


6. Click the **Search (**) button.

4. The search results display as the snapshots of the associated video clips. Click to playback the video clips with activities in the detection zones.

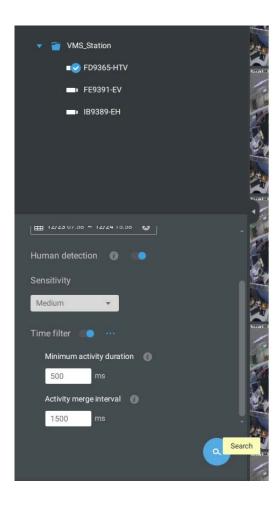
Hover the screen with your mouse, and the length of each video clip is displayed.

Note that unless interrupted, the playback continues with all detection zone clips, by continuing to the successive clips.



Smart search II is available only for newer line of cameras that come with Smart Motion detection and other Smart VCA features. Smart search II has the following benefits:

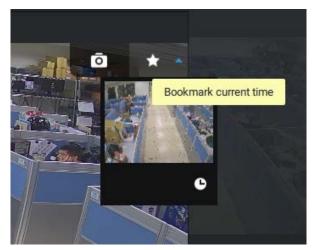
- Faster search: Metadata is saved with videos coming from the cameras running Smart VCA detection. With the help of the metadata, the search focuses on the effective alerted vectors and the adverse effects, e.g., headlights causing dramatic contrast or small animals passing through, have already been eliminated by the camera. The search can be more rapidly completed.
- 2. People detection: The search can be conducted for human activities only. Activities matching the silhouettes of human will be considered as effective results.
- 3. Multiple-point polygon: Users can select a region of interest by drawing a easily-configured polygon. In addition to the pre-configured detection rules on VCA cameras, users can create their own Smart VCA Detection rules on the VAST search panel screen.



You can specify the time span, People detection, Sensitivity level, and time filter parameters in a Smart Search II panel. 5. You can then click to open any clip of your interest. Each marked event clip will be indicated by a lighter color on the time line. Select and double-click on a video clip, and then right-click or select the bookmark or snapshot functions from the upper-right.



Move your cursor to the upper right corner of the playback window to display the Snapshot and Bookmark buttons. Use them to configure the current play time as a bookmark or take a snapshot.

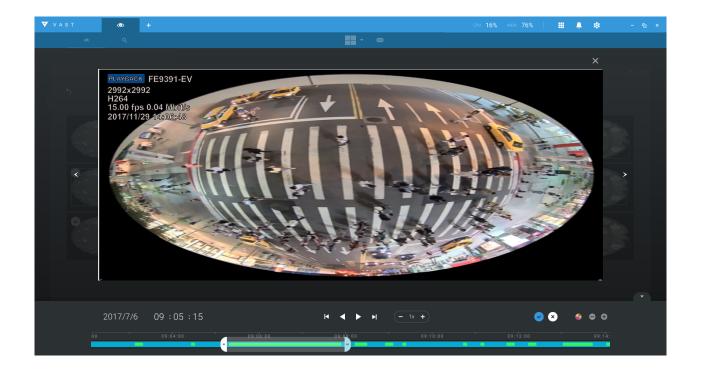


While in the full-screen Playback window, you can right-click to select or deselect the display elements including motion cells, tracking block, and tracking dot.

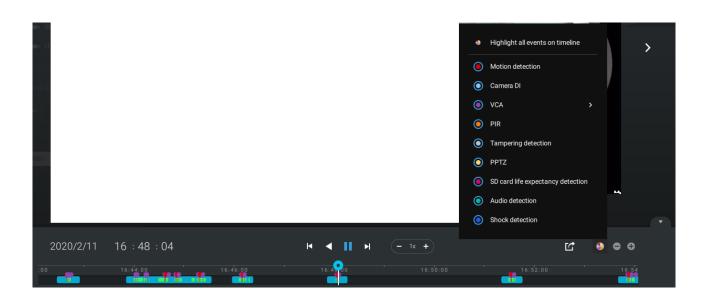
	Bookmark	Ctrl+Shift+B				
	Snapshot	Ctrl+Shift+C				
~	Show motion cells					
~	Show tracking block					
~	Show tracking of	dot				

 If you find important events, use the Export function to mark the start and end points on the timeline to export a video clip. Use the pull tabs on time line to determine the export length. By default, the export length is 2 minutes long.

The playback control in the Smart search window is identical to that on the Playback window.



Different events on the timeline are indicated by tags of different colors. Click on the event highlights button to verify their colors.

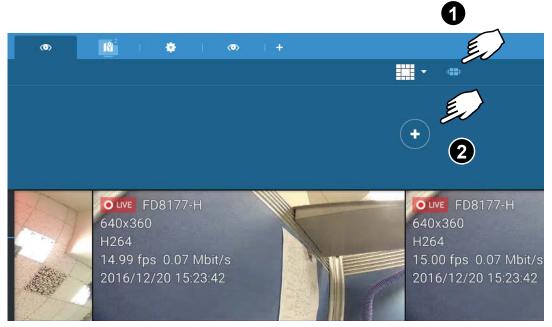


2-2-17. Tour

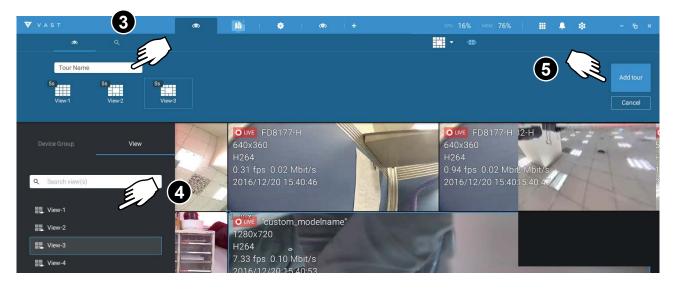
A tour can be configured to consecutively display multiple views. A tour allows users to quickly glimpse through many view cells in a timed pattern. As a tour can contain multiple views, you should design and configure camera views before configuring a tour.

To configure a tour,

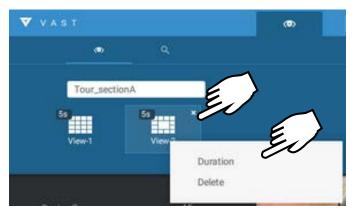
- 1. Click on the Add a camera tour 💷 button.
- 2. Click the Add button.



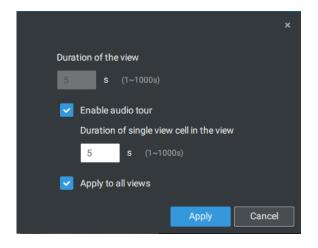
- 3. Enter a name for the tour.
- 4. Single-click to select a view. Select multiple views each by a single click.
- 5. Click the Add Tour button.



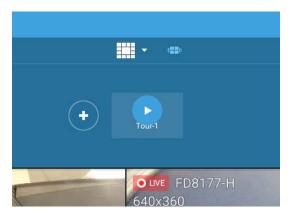
The default for the duration of the display of each view is 5 seconds. You can right-click on each view to display the Duration of each view. You can apply the same duration of all views, or allow each view to display on screen for a different span of time.



You can enable the **Audio tour** option which plays the audio inputs from each view cell for a specific period of time.



Mouse over a configured tour, and then click to start a tour.



When playing a tour, and you want to stop the tour, you can left-click or right-click on the screen. Click the Tour icon again to return to the singular live view.

2-2-18. Thumbnail search

The Thumbnail search function is like doing a post-production editing in film making. Screens from across different time spans are shown to facilitate the search for evidence.

Click on the Thumbnail serach button to enter the Thumbnail search window. The default time span is 100 minutes, starting an hour earlier of the current system time.

To use Thumbnail search,

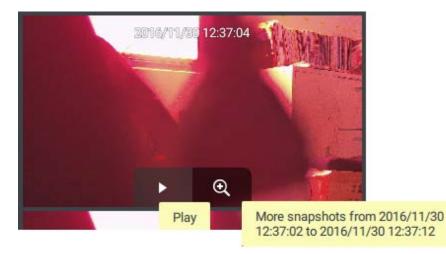
- 1. Use the date and time selectors to specify a time span during which you suspect the event of your interest has occurred.
- 2. If preferred, tune the interval and clip size. The default length for each clip is 10 seconds.
- 3. If you find a clip might contain an event of your interest, you can click to select, and then slide left and right to watch the activities within.



4. Hover your cursor to the lower center of a clip to display the Play and the More snapshots options. If you click More snapshots, another window will prompt to display all frames within the clip.

When you select to display the clip details (specific time span), the time span and the interval information will change accordingly.

When you find an event of your interest, you can play that video clip and use the export function on screen to output the evidence. You may also place a bookmark on the timeline.



Chapter 3 Applications: 3-1. I/O DI/DO Devices: IO Box and Related Configuration

Use the software utility that comes with the IO box, e.g., Advantech's Adam/Apax.NET utility, to configure IP address, and test the DI/DO connectivity. The connections to external devices should be completed before configuration on the software.

Advantech Adam/Apax .NET Utility (Win32)	Version 2.05.10			
File Tools Setup Help				
🕒 🔄 e. 📲 🖌 🐌 🕨 🔯				
COM3 Branet 152.166.6.117 COM3 Provide Grup COM3 COM3 COM3 COM3 COM3 COM3 COM3 COM3	Setting Network setting: MAC address: IP address: Subnet address: Default gateway:	[00-D0-C9-P0-EF-3В [192.168.6.118 [255.255.0.0 [192.168.6]1	Apply change	
ADAM/APAX				

Enter Settings > Device > DI/DO Device. Click the add I/O button on top.

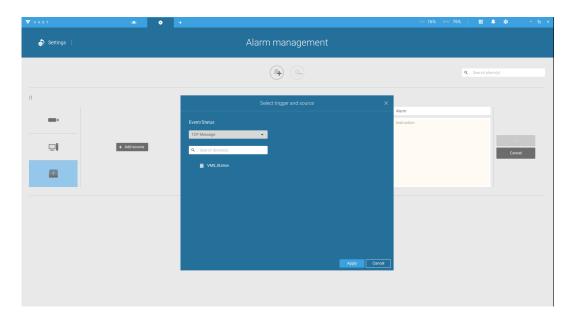
V A S T	@ 0	+	ere 16	% HEN 76% 🗏 🗍 🌲 🏟	- 6
🔊 Settings		I/O Box			
Cameras Emilia Recording options Sites	(V0) (V0) Q. Startch devices(s)	Edit I/O Box Devicename ADAM Band Advantech ADAM40022 IP 192.164.6.118 = 502 Username Password eccence			
Pos	1 D14 1 D15	Di number: 8	DO number: 8		
I/O DI/DO devices	DI 7 DI 8	1 DI1 1 DI2	0 D01 0 D02		
	0 D01 0 D02 0 D03	0 D13 0 D14	0 D03 0 D04		
	0 D0 4 0 D0 5	0 DIS 0 DIS	0 D05 0 D06		
	0 D06 0 D07	1 DI 7	0 007		

Enter the I/O box's IP addess and credentials, and select the correct model name from the pulldown list on the right. Click the **Apply** button to proceed. The current I/O connections are also displayed on screen, such that the status is displayed when DI pins are connected to detection devices.

Configuring I/O Box DI/DO as a Trigger or Action in Alarm

Enter the Settings 🌞 > Alarm window. Click the Add alarm 🕒 button on top.

Select the External Device event 🔛 , and then click the Add trigger + Add trigger button.



The Select trigger and source window will prompt.

Select either the I/O Box DI or DO as the triggering source.

	Select trigger and source
Event/Status	
TCP Message	▲
I/O Box DI	
I/O Box DO	
TCP Message	
VMS_Station	

Select one or multiple DIs as the triggering source and click the **Apply** button.

Select trigger and source						
Event/Status	ADAM					
I/O Box DI 🗸						
Q Search device(s)	✓ DI 1 DI 2					
VMS_Station	DI 3					
VO ADAM	DI 4					
	DI 5					
	DI 6					
	DI 8					
		l				
		-				
	Apply C:	ancel				

Click Add action + Add action, and select a corresponding action, such as sending live streaming, record videos, trigger a DO, sending an HTTP request, or sending an Email. When done, click the Add button.

	Select actions		×
Send live streaming	•		
	_		
Q Search device(s)			
VMS_Station			
"custom_modelname"			
🗹 💻 FD8177-Н			
FE9182-H			
SD9366-EHL			
■ IP8166			
		Add	Cancel

Configure a schedule during which the Alarm configuration will take effect. If no special time span is needed, you can simply select Always.

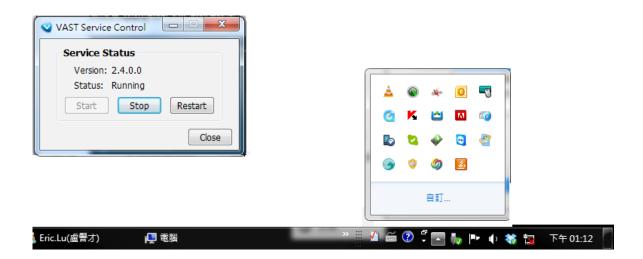
	Add a schedule template							
	te name Offi	ce						
00:00	Sun	Mon	Tue	Wed	Thu		Sat	
01:00								
02:00		00:00~23:30						
03:00								
04:00								
05:00								
06:00								
08:00								
09:00								
18:00								
19:00								
20:00								
24:00								
							Add Cance	1

Enter a name for your Alarm, and add description for your configuration, e.g., "intrusion detected on the front door." When done, click the Add button. The Alarm configuration takes effect immediately.

V AST 💿	•			eru 16% M	🕬 76% 🔠 🌲 🏘	- 6 ×
مُ Settings		Alarm ma	nagement			
		-			Q. Search alarm(s)	
If	Do		At			
			+ Add a s	Alarm		
-			Always	Instruction		
			Customize			AU
+ Add source	+ Add a	ction	✓ Office			Cancel
No. Name	If the following is triggered	Ву	Do	On/to	At	
1 Alarm	ADAM DI 1	I/O Box DI	Send live streaming	FD8177-H	Office	

NOTE:

If an I/O module is started later than the VAST server, you may not be able to access the I/O module. You should then re-start the VAST service.



3-2. Configuring Redundant Servers - Failover

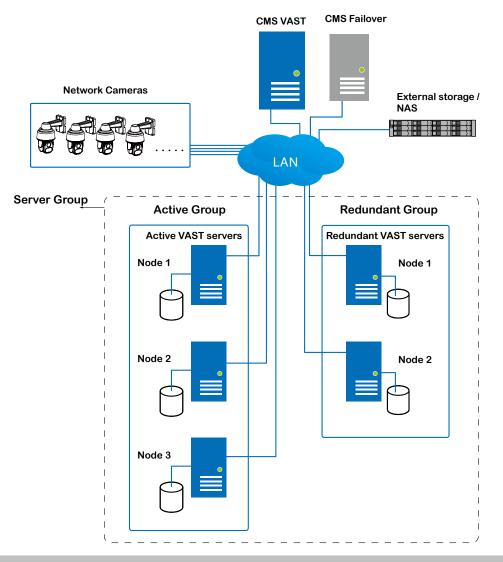
VAST2 servers can be configured into two groups: Active and Redundant. The Active group performs daily recording and monitoring tasks, while the Redundant group acts as the standby servers. In the event of server failures, the Redundant group becomes active, and takes over the recording task.

The Redundant server group configuration consists of the following:

- 1. One VAST2 server designated as the **CMS** (Central Management server) VAST central management server. Another VAST server can serve as a CMS failover server.
- 2. At least one VAST2 server in the **Active** group.
- 3. At least one VAST2 server in the **Redundant** group.
- 4. Gb/s network or higher-speed connections among the servers. All Active and Redundant groups can reside in different subnets, provided that static IPs are configured for these servers.

IMPORTANT:

For a Redundant server configuration, you must first enlist VAST servers in the **Sites** configuration page before configuring the Redundant server groups. See the **Sites** configuration page.



Below are the definitions of server roles:

- 1. **CMS** VAST server: The main access portal for the configuration.
 - 1-1. CMS server is where the **Failover** configuration takes place.

1-2.	CMS continuously polls to check the hearbeats to monitor the statuses of all Active
	and Redundant servers.
1-3.	CMS regularly backs up the configurations on Active servers.

- 1-4. CMS assigns redundant server(s) to the takeover of a failed Active server.
- 1-5. In a Redundant server configuration, the CMS is supposed to be up and running at all time. If the CMS server fails, the server failover and failback operation will not take place. It is therefore preferrable to configure a CMS redundant server, and install the CMS server at a high up-time environment, such as on a VMWare configuration.
- 2. **CMS Redundant** server: This is a failover server that serves as the backup for the CMS server.

Note that this redundant server is configured in **Settings** > **Devices** > **Sites**. Click **Add Sites**, and select "Add as a redundant server for" "CMS." See next section for the configuration procedure.

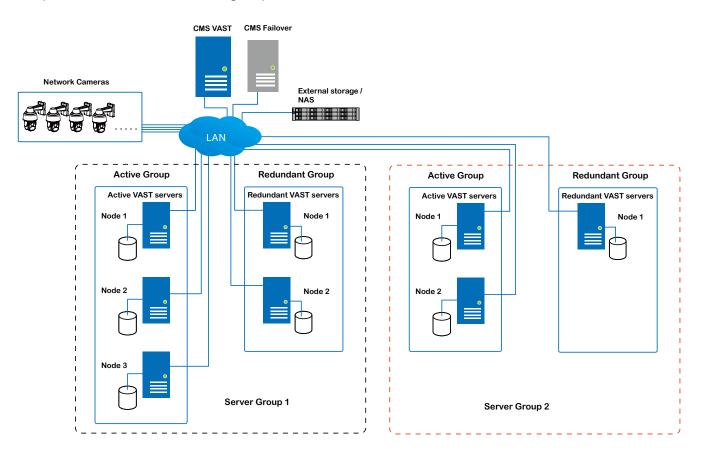
VAST2	o 🕸 +		cra 10% Mich 16% 🏭 🌲 🏟 — 🖻 × 1
🔊 Settings		Device management	
Cameras Sites POS D/DO devices D/DO devices Cata magnet External devices	C Sech device Image: Contract device <td< th=""><th>New sites sarch IP/Domain name 192.168.5.132 Pr 3443 CMS password CMS @ Subsations CMS POP main name CMS POP 3443 Back up data after network is disconnected for 30 sconds (5-3600) Windows account (options) Host Des name Des name Des name</th><th></th></td<>	New sites sarch IP/Domain name 192.168.5.132 Pr 3443 CMS password CMS @ Subsations CMS POP main name CMS POP 3443 Back up data after network is disconnected for 30 sconds (5-3600) Windows account (options) Host Des name Des name Des name	

- 3. **Active** servers: Active VAST servers are the work horses that perform recording and monitoring tasks.
- 4. **Redundant** servers: The Redundant servers are actually active-standbys. They participate to continue video recording in the event of active server failures. It is recommended for the Redundant servers to have an equivalent or higher processing power than the Active servers. The same applies to the size of storage volumes and the disk drives' write performance.

Note that you cannot configure a Redundant server by opening a local console.

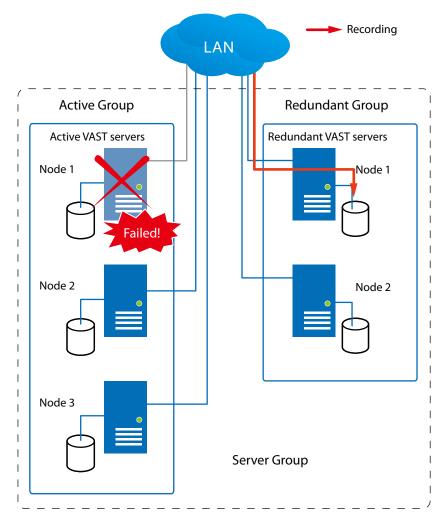
The conditions during the failover process are illustrated below:

Multiple Active and Redundant groups can be created.

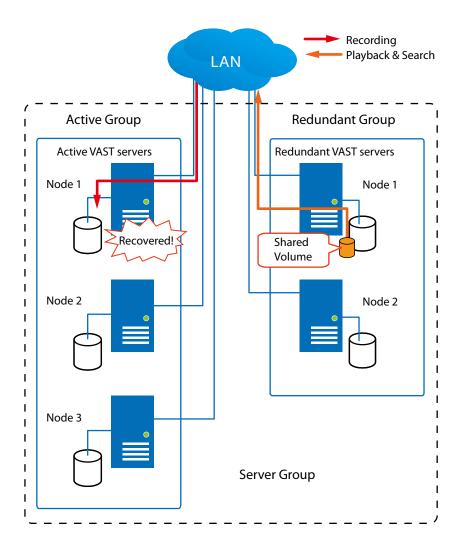


Each Redundant server can serve as the backup for ONE Active server. Depending on the number of the Active and Redundant servers, if the number of failed servers exceeds the number of Redundant servers, the failover will be abandoned. For example, if 2 Active servers failed, and there is only 1 Redundant server available, the second Active server that failed will be abandoned.

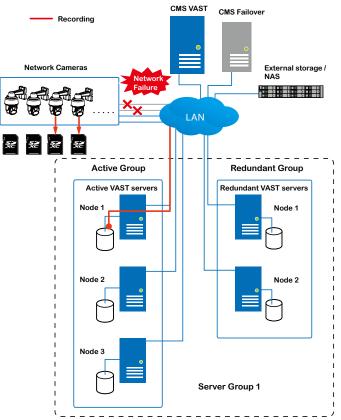
In the event of a server failover, a VAST2 server in the Redundant group takes over the recording task. Note that depending on the network environment, the takeover can take up to 5 minutes.



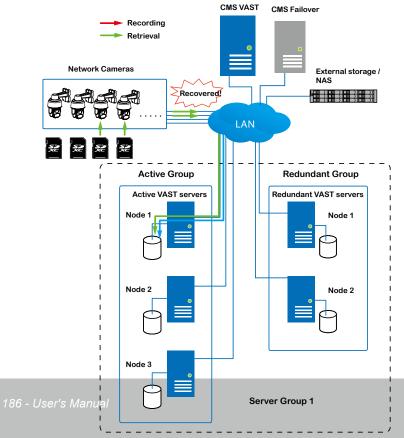
Once the server in the Active group is restored to normal operation, and a CMS server requests for the recordings and data occurred during the time the active server failed, the requests will be fulfilled by a shared volume on the redundant server. Due to the concerns with network bandwidth and processing power, the restored active server does not synchronize its recording pool with that on the redundant server after the failover and failback process.



In terms of network failure, the VAST2 configuration supports Seamless Recording. For cameras equipped with an SD card, video is recorded to the SD cards in the event of network failure. Of course, the cameras must have a backup power source, such as a DC 12V input. In cases such as the only PoE switch or PoE mid-span fails, power is lost.



Once the network connection is restored, the VAST2 servers resume the recording task and also retrieve video segments from the SD cards. The video segments recorded during the network failure will be stitched up with those occurred before and after the network failure. The retrieval speed varies depending on the available network bandwidth and CPU resources.



To enable Seamless recording, find the associated option in **Settings** > **Recording options**, and select the Seamless recording checkboxes. Camera models that support the Seamless recording option will have it listed.

VAST2	\$								CPU 10% MEM 64%	III 🌲 🏟 — 🕫
🄊 Settings			Re	ecording mar	nage	mer	nt			
Recording options		MS_Station DefaultGroup	Archive name	efaultGroup 16			VMS_Station 100.1 GB			
Failover			Storage + New st	orage						Recycle Options
Local DB				cameras						
			Name	IP	Stre	aming	Schedule		Seamless recording	Activity Adaptive Stream
			All cameras	10.17.2.49	1		Continuous	*		
			IB9367-EH	192.168.4.179	1		None	*		
			FE8191	192.168.4.168	1		None	*		
			FD8377-HTV	192.168.4.128	1		None	*		
										Cancel

Failover Configuration Process

Before Failover configuration, you need to add other servers to your Failover configuration. Below is a screen from the Sites management window.

- If you are adding a Redundant server, select the "Add as a redundant server" checkbox, for either a CMS server or VAST Substations.
- If you are adding a server without selecting this checkbox, it will be considered as an **Active** server.
- When adding a Redundant server, you can provide a Windows account 802.1x domain user name and password. A Redundant server requires this because a full access to the recorded data is required during the failover and failback process.

VAST2	\$ +	сеч 9% мем 66% 🏭 🌲 🏟 — Ба 🗙
🔊 Settings	Device management	
Cameras Sates DrO DrO devices Co Data magnet External devices	Adveces New Sites MS.Sation ND9322P New Sites IP/Domain name D2322P Ad as a redundant server for Ad as a redundant server for Add as a redundant server	K

When the "Add as a redundant server" checkbox is selected, enter the name of your Windows domain and the user credentials for a full access to the Redundant server.

Site m	nanagement	
New sites Search		
IP/Domain name	SSL only	
CMS password	CMS Substations	
Windows account (optional)	Host	
	User name Password	
		Add Cancel

Note that it is a must for the Redundant server to be installed differently by selecting a "**Redundant server**" checkbox during the installation process.

VIVOTEK VAST2 Installation
Select a server
 Standard server Free version: 32 channels of VIVOTEK camers only Trial version: 256 channels of camera licenses and advanced licenses for 60 days Redundant server
< Back Next > Cancel

When a Redundant server is successfully added, the server will be listed under your VMS station.

	Name VMS_Station_R		
Q Search devices	Disable this redundant serve	er.	
VMS_Station			
VMS_Station_R	Windows account (optional)	VIVOTEK	0
		eric.lu	
	.		
A Redundant server comes with a	n associated icon, 🔂		

An Active server must have a CMS password configured for the hierarchical configuration.

Note that on the **Active servers**, you should configure them as the subordinates to your CMS VAST server. On a web console to these servers, open the Site management page, and select **"Allow CMS to access this site**." Create a common password for the CMS hierarchy.

▼ VAST: 00 12 +	
🔊 Settings	Site management
Carneras Carneras Sites FOS L/O D/DO devices	Name VMS_Station Port 3443 SSL only Model VAST CMS ✓ Allow CMS to access this site Image password For CMS connection only

Two agents will be running on the Active and Redundant servers, "stunnel" and "VMSWebServer." Make sure they are not blocked out by your firewall. These agents can be found in the default folders below:

C:\Program Files (x86)\VIVOTEK Inc\sTunnel\stunnel.exe C:\Program Files (x86)\VIVOTEK Inc\VAST\Server\VMSWebServer.exe

 	Allow apps to communicate through Windows Firewall To add, change, or remove allowed apps and ports, click Change settings. What are the risks of allowing an app to communicate? Allowed apps and features: Name Private ØSHELD Streaming NvStreamer TCP Exception ØSHELD Streaming SAS UDP Exception ØSHELD Streaming SASU UDP Exception ØSHELD Streaming SASU UDP Exception		Allow apps to communicate through Windows Firewa		~ Ō	Search Control Panel	Q
Allow apps to communicate through Windows Firewall To add, change, or remove allowed apps and ports, click Change settings. What are the risks of allowing an app to communicate? Allowed apps and features: Name Private SHIELD Streaming N-Streamer UOP Exception G SHIELD Streaming SSAU UOP Exception G Sherer G G Shore G	To add, change, or remove allowed apps and ports, click Change settings: What are the risks of allowing an app to communicate? Allowed apps and features: Name Private SHELD Streaming N-Streamer UDP Exception SHELD Streaming SAS UDP Exception Sherror Sherror Store Purchase App	Edit View Tools					
To add, change, or remove allowed apps and ports, click Change settings. What are the ricks of allowing an app to communicate? Change settings Allowed apps and features: Private Public Name Private Public Ø SHIELD Streaming NvSteamer TCP Exception Ø Ø Ø SHIELD Streaming SASU UDP Exception Ø Ø Ø ShiELP Streaming SASU UP Exception Ø Ø Ø ShiELP Streaming SASU UP Exception Ø Ø Ø ShiELP Streaming SASU Ø Ø Ø Ø ShiELP Streaming SASU Ø Ø Ø Ø ShiELP Streaming SASU Ø Ø Ø	To add, change, or remove allowed apps and ports, click Change settings: What are the risks of allowing an app to communicate? Allowed apps and features: Private Public Name Private Public SHELD Streaming NvStreamer TCP Exception Image: Communicate Public SHELD Streaming SAS UOP Exception Image: Communicate Public SHELD Streaming SAS UDP Exception Image: Communicate Public Sher Server Image: Communicate Public Shore						
To add, change, or remove allowed apps and ports, click Change settings. What are the ricks of allowing an app to communicate? Change settings Allowed apps and features: Private Public Name Private Public Ø SHIELD Streaming NvSteamer TCP Exception Ø Ø Ø SHIELD Streaming SASU UDP Exception Ø Ø Ø ShiELP Streaming SASU UP Exception Ø Ø Ø ShiELP Streaming SASU UP Exception Ø Ø Ø ShiELP Streaming SASU Ø Ø Ø Ø ShiELP Streaming SASU Ø Ø Ø Ø ShiELP Streaming SASU Ø Ø Ø	To add, change, or remove allowed apps and ports, click Change settings: What are the risks of allowing an app to communicate? Allowed apps and features: Private Public Name Private Public SHELD Streaming NvStreamer TCP Exception Image: Communicate Public SHELD Streaming SAS UOP Exception Image: Communicate Public SHELD Streaming SAS UDP Exception Image: Communicate Public Sher Server Image: Communicate Public Shore						
What are the risks of allowing an app to communicate? Change settings Allowed apps and features: Name Private Public Ø SHIELD Streaming NvStreamer TCP Exception Ø Ø SHIELD Streaming SSAS UDP Exception Ø Ø Shiel SAN UPP Exception Ø Ø Shiel SAS SAN UPP Exception Ø Ø Shiel SAS UPP Exception Ø Ø Shiel SAS UPP Exception Ø Ø Shiel SAS UPP Exception Ø	What are the risks of allowing an app to communicate? Change settings Allowed apps and features: Private Public. If SHELD Streaming NuStreamer TCP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Exception If SHELD Streaming SAS UDP Excep		To add, change, or remove allowed apps and ports, click Change setti				
Allowed apps and features: Name Private Public Ø SHIELD Streaming NvStreamer TCP Exception Ø Ø Ø SHIELD Streaming SAStreamer UDF Exception Ø Ø Ø SHIELD Streaming SAStreamer UDF Exception Ø Ø Ø SHIELD Streaming SASA UDF Exception Ø Ø Ø SHIELD Streaming SSAU UDP Exception Ø Ø Ø SHIELD Streaming SSAU UDP Exception Ø Ø Ø Shift Prap □ □ Ø Shift Prap □ □ Ø Store Ø Ø	Allowed apps and features: Name Private Public SHIELD Streaming NvStreamer TCP Exception Image: Comparison of the compar						
Name Private Public IS SHIELD Streaming NvStreamer ICPE Exception IV IS SHIELD Streaming SvSteamer UDP Exception IV IS SHIELD Streaming SSAU UDP Exception IV IS ShiMP Trap IV IS Shife Store IV IS Store IV	Name Private Public Ø SHELD Streaming NvStreamer TCP Exception Ø Ø Ø SHELD Streaming NvStreamer UDP Exception Ø Ø Ø SHELD Streaming SSAU UDP Exception Ø Ø Ø SHELD Streaming SSAU UDP Exception Ø Ø Ø SHELD Streaming SSAU UDP Exception Ø Ø Ø SMIED Streaming SSAU UDP Exception Ø Ø Ø SmartScreen Ø Ø Ø Sh Server Ø Ø Ø Store Purchase App Ø Ø Ø Store Purchase App Ø Ø Ø Store Purchase App Ø Ø		What are the risks of allowing an app to communicate?	Cha <u>ng</u> e settings			
Image: SHIELD Streaming NvStreamer TCP Exception Image: Streaming NvStreamer UDP Exception Image: Streaming Streamer UDP Exception Image: Streaming Streaming SSAU UDP Exception Image: Streaming Streaming SSAU UDP Exception Image: Streaming Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Exception Image: Streaming SSAU UDP Except	Image: Streaming NvStreamer TCP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streaming SASU USP Exception Image: Streamin		Allowed apps and features:				
Ø SHILD Streaming NASteamer UDP Exception Ø Ø SHILD Streaming SASA UDP Exception Ø Ø SHIELD Streaming SSAU UDP Exception Ø Ø SmatScreen Ø I SNAW P Trap I I Sh Server Ø Ø Store Ø	Ø SHED Streaming N-Streamer UPD Exception Ø Ø SHELD Streaming SSAS UDP Exception Ø Ø SHELD Streaming SSAS UDP Exception Ø Ø SmartScreen Ø Ø SmartScreen Ø Ø Sh Server Ø Ø Store Purchese App Ø Ø Store Purchese App Ø Ø store Purchese TLs efficienting proxy Ø		Name	Private Public ^			
Image: Set Subset of Set Subset of Set	Ø SHELD Streaming SSAS UDP Exception Ø Ø SHELD Streaming SSAU UDP Exception Ø Ø SmartScrean Ø S ShMP Trap 0 Ø Sh Server Ø Ø Store Purchase App Ø		SHIELD Streaming NvStreamer TCP Exception				
Ø SHILD Streaming SSAU UDP Exception Ø Ø SmartScreen Ø D ShMP Trap D Ø Sh Server Ø Ø Store Ø	Image: Shift DD Streaming SSAU UDP Exception Image: Shift DD Streaming SSAU UDP Exception Image: Shift DD Streaming SSAU UDP Exception Image: Shift DD Streaming Stre						
Ø SmartScreen Ø SNMP Trap	Ø'SmartScreen Ø'Ø' SNMb Tap Ø'Ø' Ø Sh Server Ø'Ø' Ø Store Ø'Ø'						
□ SMMP Trap □ □ Ø Seh Server Ø Ø Ø Store Ø Ø	SNMP Trap Image: Comparison of the system of the syste						
Ø Sah Server Ø Ø Store Ø	Ø Sah Server Ø Ø Store Ø Ø Store Purchase App Ø Ø stunnet – TLS offloading and load-balancing proxy Ø Ø Skuther Ø						
🗹 Store 🖌 🖌	Store Store Purchase App Stunnel - TLS offloading and load-balancing proxy Stunnel - TLS offloading and load-balancing Proxy Sturmer Stur						
	G Store Purchase App G Supre La Store Purchase App G stunnel - TLS officialing and load-balancing prox G SturPTP G G G G C Store Provided G SturPTP G G G G G G G G G G G G G G G G G G G						
	 ✓ stunnel - TLS offloading and load-balancing proxy ✓ ✓ SXUPTP ✓ 						
	SXUPTP V						
M Take a Test			✓ Take a Test				
Details Remove	Details Remove			Details Remove			
				Allow another app			
Allow another ann	Allow another ann			riter enteriner oppin			
				Allow another app			
Allow another app	Allow another app						

Click on the Add Dutton to create a Redundant server group. The Active and Redundant servers you enlisted on the Sites page should all be listed below. Select the members of the Redundant group, and click Add to complete.

The default for the network disconnection timeout is 30 seconds. It is not recommended to configure a very short timeout, e.g., 5 seconds, because if doing so, a temporary network disorder can make servers consider the Active server(s) have failed.

V A S T	ത ജ് +		cru 16%, мом 76%, 🏛 🌲 💠 – 🕤 ×
🔊 Settings	:]	Failover	
Recording options Backup Failover	Image: A second property and a seco	Croup name Failover group	Search servers Search servers Search servers
		Back up data after network is disconnected for 30 seconds. (5~3600)	Add Cancel

3-3. VCA (Video Content Analysis)

The VCA Report utility is started from the tool bar on top, C. The VCA Report utility provides comprehensive graphs and line charts for quick access to the data collected through VIVOTEK's People Counting modules, such as the SC8131 stereo camera. Statistical results is refreshed by hour or minutes, and you can compare the results acquired through different time periods or among different surveillance areas. These data help figuring the customer flow in retails so that shop owners can optimize the arrangement of store layout, or mange queues more efficiently.

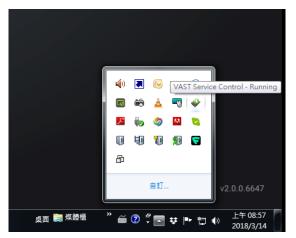
Note that the configuration of detection methods in People Counting still occur on a web console to individual cameras. It is not configurable through the VAST LiveClient.

Prerequisites:

The prerequisites for using the VCA Report are:

1. The monitoring server running the VCA Report utility must be up and running during the time the counting VCA is taking place. If you power off the server, the counting metadata generated during the server down time will not be available for analysis.

The VAST2 server instance runs in the background. The VAST2 management console needs not be started during the VCA Report data collection process.

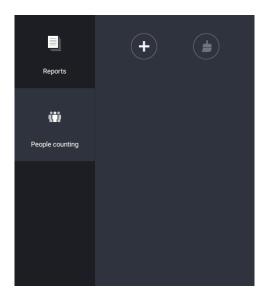


 Cameras running the VCA utilities have been configured and added into the VAST deployment. The instances of available VCA rules will be listed in the Area panel.

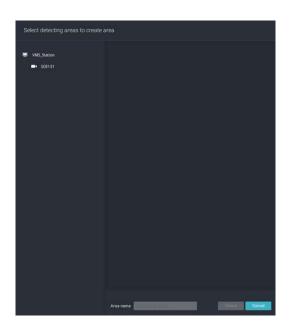
- **3.** The life expectancy of VCA records is 5 years.
- **4.** Currently the utility supports Windows XP, 7, 8, and 10.
- 5. The latest revision VAST supports Seamless Recording, in order to retrieve collected data and recording during Ethernet disconnection. Provided that an SD card is installed on the VCA-enabled cameras, the VAST station gradually retrieves data from the SD card after the connection is restored.

To start VCA report:

- 1. Click on VCA report 🗠 button on the tool bar.
- 2. Select People Counting.
- 3. Click on the Add area + button.



4. Select a camera that is VCA-enabled, and then click the Create button.

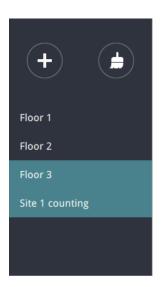


5. The pre-configured counting rules (areas) will automatically display. Select a counting rule and enter a name for the area. When done, click the Create button.

Select detecting areas to create a	area	
♥ VMS_Station ■ SC8131	SC8131 In our Due out Counting1 FlowPathCounting1	
	Area name Corridor	Create Cancel

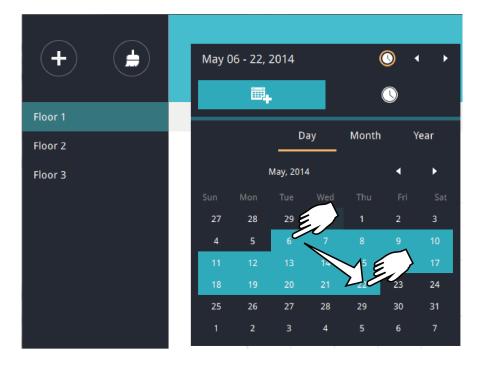
If only one camera is selected, its name will apply as the Area name. If not, enter a name for the area.

6. Click to select one or multiple areas. Those selected will be highlighted in a different color.



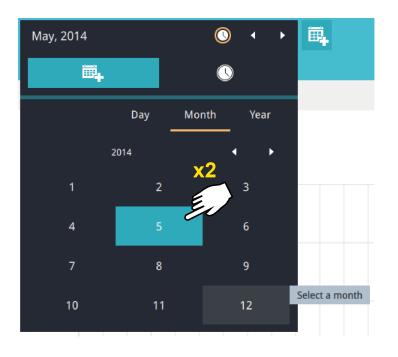
7. Select Date & Time

- 7-1. By default, the time displayed on the calendar is the current system time on the client computer running the utility. Select from the **Date** selector on top.
- 7-2. Select a date or span of time from the calendar or use the **Time** selector to select a span of time.
- > Single-click to select a date or click and drag to select multiple dates.
- > You can select a month or a year using a single click. If you select a month, the timeline unit will be days within the month. If you select a year, the timeline units will be the months in a year.
- In the Month or Year panel, single click to select the entire month or an entire year. Doubleclick to select sub-units, e.g., days within a month. If you double-click on a Month panel, you will enter the Day panel.



You can select a different month in the **Month** or **Year** panels. The **Calendar** panel disappears if left unattended for 2 seconds.

On a **Month** panel, double-click to select a month, and the **Day** panel for that particular month will display.



Note the following when making the configuration:

- When a date is selected, the Date and Time panel will not automatically close, and the configuration changes will not take effect until it is closed. You can click on the outside of the panel to leave the panel.
- You can select multiple days to form a span of time. Select one date with a single click and select multiple dates by draging your cursor across the screen to a preferred end date.
- To select a year, click to open the Year panel. Single click to select a year. Multiple years can be selected using the click and drag method.

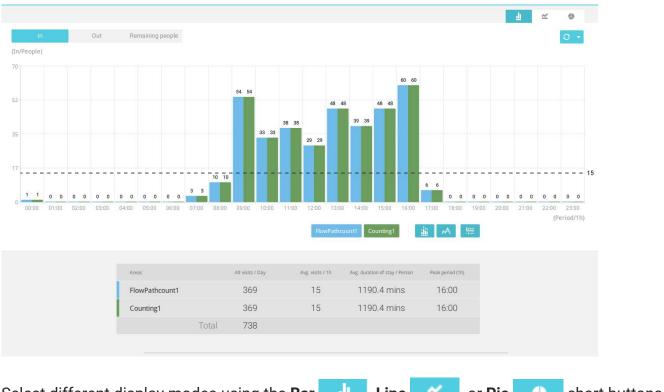
7-3. Select the hours to be included in the statistical poll using multiple clicks on the chart.

Single-click to select an hour or click and drag to select multiple hours.

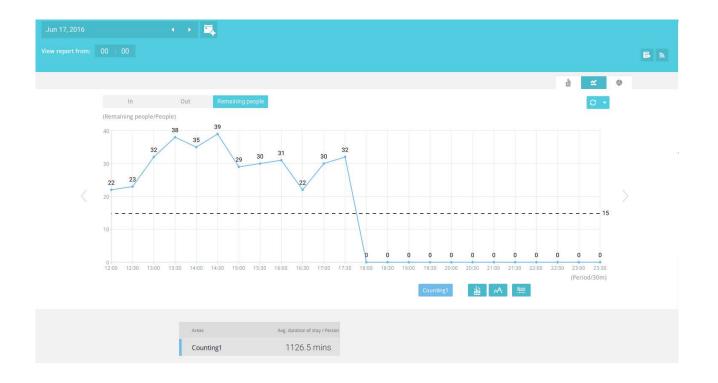
Jan 31 - Feb 09, 2015	()
≣ ₊	3
00:00 01:00 02:00 03:00 04:00 05:00 06:00 07:00 08:00 09:00 10:00 11:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00	Selected 00:00 - 23:00

Note that you can only compare the counting results from two spans of time if you select only one Area. If you selected multiple Areas, you can not compare the results from multiple time spans.

7-4. Click outside the Calendar panel. The statistical results will display. The default display is the bar chart. Below is a sample screen showing the results polled from 3 areas. Up to 8 areas can be selected in one view.







Note that the timeline units can vary depending on the span of time you selected on the Calendar panel. If a date was selected, hourly data will display in chart. If a year was selected, monthly data will display in chart.

Use the following functional buttons to change the display parameters

Show data on chart

i Displays the collected numbers on chart.

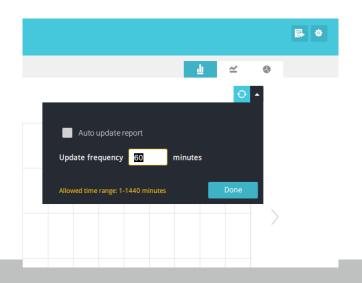
Average 🕂 : Displays the average number per time span unit (e.g., per hour). If the interval

is changed to 30 mins, the average number will be halved comparing to the number acquired by every hour.

Report Interval : Configure the intervals for polling data from the camera. The default for displaying results is by every hour. If you enter 30 minutes as the display interval, all data will be listed on the basis of the 30 minutes time span. The configurable range is 1 to 1440 mins.



You can use the update menu on the side of the Refresh button to determine an automatic update schedule. You can let the statistic chart update itself by a regular interval.

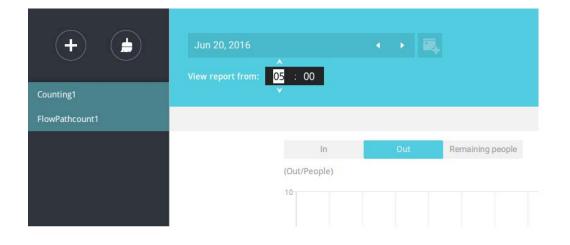


If you selected only one area, you can use the Shift key to select multiple areas (or two spans of time). You can select multiple dates in the Calendar panel.

Use the **Refresh** button ^C to poll the latest data from camera.

0

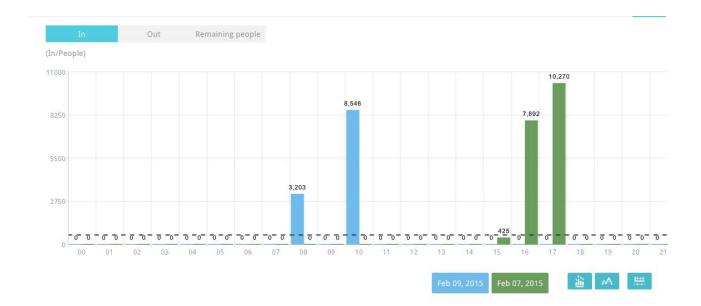
Use the time selector on the **View Report from** pane to select the start time of your statistics view window. Data collected before that time will not be displayed.



A number is displayed when you mouse over an area on the chart. Move your cursor to an area on chart, and the number is displayed.

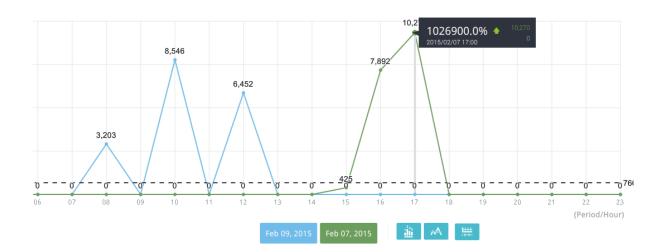


Data on a time line will be generated. To close the window, use the close button on the second date information. Equivalent spans of time can also be used for comparison. For example, you can compare the data in a span of 4 days against another span of 4 days.

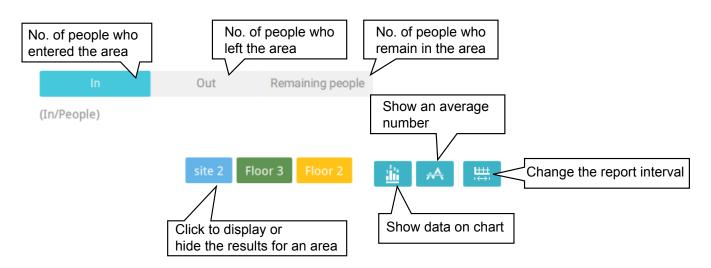


Note that the Compare function only applies when you select to display only one area on screen.

In a comparison result displayed in a line chart, mouse over to the peak value to display the percentage of an increase or decrease rate.



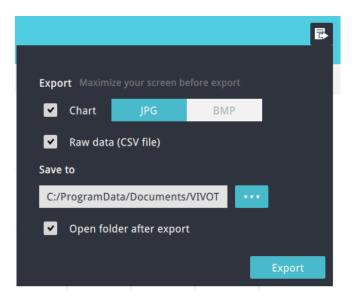
See below for the functions of buttons on screen.



In addition to the charts, a summary of displayed data will be listed below showing the areas involved, visits/Day or Month, Average visits / Hours / Days, Average duration of stay / person, and the Peak hour.

Areas		All visits / 4 days	Avg. visits / Day	Avg. duration of stay / Person	Peak day
Floor 3		490,870	122,718	106.3 mins	12/04
Floor 2		959,482	239,870	105.9 mins	12/02
site 2		3,873,510	968,378	108.0 mins	12/01
	Total	5,323,862			

8. When done with displaying the results, you can use the **Export** button to produce an image file to preserve the current results. Both a spreadsheet and a graphic chart will be produced.



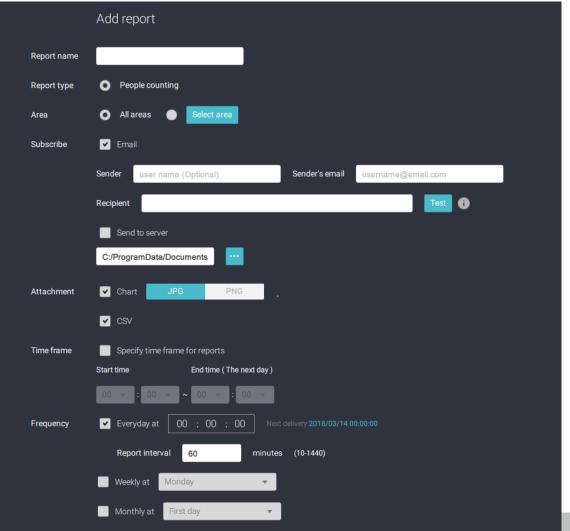
By default, the exported report is placed in:

C:\ProgramData\Documents\VIVOTEK Inc\ VAST\Client\VCAReport Click the Reports Subscription button to configure the regular report sent to your Email account or a specific location on the server itself.
 Select the following:

1.	Report type: People counting results, or Heatmap (Heatmap does not produce CSV file)
2.	Area: All areas or a preconfigured area.
3.	Subscribe: Enter the sender and recipient Email addresses. You can also configure to
	send the report to a specific location on the server.
4.	Attachment: Select to attach graph Charts in JPG or PNG, and the CSV data files.
5.	Time frame: Select the time coverage of the report, during which data is collected.
6.	Frequency: Specifies when and how frequently to deliver the reports.
L	

Select the time to deliver your mail notification. Enter valid Email addresses as the sender and receiver addresses and make sure the SMTP mail server configuration has been properly configured on your VAST server. This VCA mail notification utilizes the mail service on VAST for regular notification. You can then receive Email notification every day on your Email account. You can enter up to 5 recipient addresses.

Select the report interval to determine how often you receive an aggregated report.



User's Manual - 203

Note that the notification contents is your current field of view, including a Bar, Line, and Pie chart combined into one image file. The In/Out/Remaining results will be generated into 3 charts. Each Area will generate one CSV file, and each CSV data file will contain In/Out/ Remaining/Summary information.

The generated file names will look like this: 20160226_test02_Remain.jpg for charts and 20160226_Summary.csv for CSV files. The Email subject will be "VCA Daily Report - 2016/02/26."

Note that if you manually export a report, the default is sending the data collected until one hour before the manual export. For example, if you generate the report at 14:07, the report will only cover the data collected until 13:59. You may use the Refresh button to manually generate immediate data inputs (those occurred between 14:00 and 14:07).

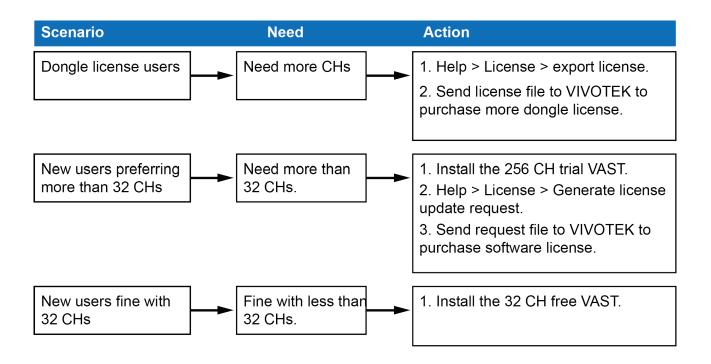
You may configure to receive regular VCA report as Weekly or Monthly using the associated menus.

Below are the messages with the Email test function.



3-4. VAST Software License

To activate the software, refer to the flow chart below:



The VAST software provides 32 free channels. Since revision 1.11, the VAST software is activated using a software license instead of the original hardware dongle.

For users running the previous dongle version, there is no need to upgrade their original license. If they need the license for more channels, They can export their license file, and purchase more dongle licenses. For users who require more than 32 channels, they can install the 256 channel trial version first, and go to **Settings** > **System** > **License** page, and click on the **Export License** button. Send the request back to VIVOTEK to purchase more channel licenses.

	\$ +					27% 🏭	۰
Settings			System management				
0							
License			Export license Import camera license	Import MAC license			
SMTP †↓†							
Preferences	Status	Site name	# VIVOTEK cameras	# Onvif cameras Purcha	sed licenses Adva	nce Package	
eedback and bugs		Lori's CMS (192 6F)	5	0	0 Purch	ased package	
		-ND8212W	0	0	0 Purch	ased package	
		-NV9411P	0	0		ased package	
	N2					ased package	
	101				0 Purch	ased package	

When you purchased and received the official software license, use the **Import License** function to activate the official license.

When importing purchased licenses,

- 1. System will dispatch licenses to VAST stations according to hardware information,
- 2. If licenses do not match the VAST stations, you can manually select which license will be dispatched to which station.

Since VAST rev. 2.6, there is an Import MAC license option. You can select a MAC license file and manually deliver the file to one or multiple substations.

Below is a sample procedure for importing the camera licenses:

1. Continue to import the camera licenses.

VAST2 💿			194	6% NEM 51%	• III 🐥 🅸	- 16 -
🔊 Settings		System manage	ment			
() License						
SMTP 111 Preferences		Export license Import ii				
	Sta Site name	# VIVOTEK cameras	# Onvif cameras	Purchased I	Advance Pa	
Feedback and bugs	CMS	1	0	0	Purchased packa_	
	-Store 1	1	0	0	Purchased packa-	
	-Store 2	1 (MAC license excluded)	0 (MAC license excluded)	MAC license	Purchased packa-	
	-Store 3	0 (MAC license excluded)	0 (MAC license excluded)	MAC license	Purchased packa	
	Total (MAC license excluded)	3 (Free:32)	0	0		

2. When in the Import page, click the Add button to select camera licenses.

dd camera licenses, then select sites to import your lie	censes.			
		Status	Site name	Purchased licens
			CMS	0
			-Store 1	0
Drop camera licenses here			-Store 2	MAC license
or click add button			-Store 3	MAC license
Add				
15				

3. Select the target servers, click Import.

Camera licenses are bundled with hardware information. When import camera licenses, the software will automatically match the licenses with corresponding servers.

CMS.lic	8		Sta	tus Site name	Purchased licens.
			-	CMS	0 (CMS.lic
Store1.lic	\otimes		-	-Store 1	0 (Store1.lic
				-Store 2	MAC license
		Import		-Store 3	MAC license
				6	

4. When done, a successful import will be indicated.

		Status Site name	Purchased licens
		CMS	10 (CMS.lic)
		-Store 1	10 (Store1.lic)
Drop camera licenses here		-Store 2	MAC license
or click add button		-Store 3	MAC license
Add	ß		
Aug			

Updating Licenses for VAST on Virtual Machines

NOTE:

- 1. The VAST server supports the installation on VMWare, Virtual Box, Parallel, and Hyper V.
- 2. A MAC address authentication mechanism is implemented for VAST running on virtual machines.
- 3. The license requests have to be generated from the VAST2 installed on a Virtual Machine. If your configuration consists of multiple VAST servers, and one of them is installed on a virtual machine, exporting license information will generate a MAClist file. The MAClist file will be used for the VAST instances running on virtual machines.

This instruction includes:

- 1. How to Export a license request from VAST2 on a virtual machine.
- 2. How to acquire the MAC addresses of the inserted or non-inserted cameras?
- 3.Send us request files & MAC addresses (If you have multiple sites, please remember to designate grouping information, such as which MAC addresses belong to which camera deployments).
- 4. How to Import MAC licenses to VAST2?
- 5. How to buy more MAC licenses for future distribution?

1. How to export request from VAST2 on VM?

- 1-1. Install VAST2 server on a Virtual machine (usually VMware workstation full 12.1.1), or download VAST2 from VIVOTEK website.
- 1-2. Insert cameras for the VAST station(optional).Go to virtual machine, Open VAST2 > Settings > Insert cameras (You may already have more than 32 cameras inserted if you are using the trial version).
- 1-3. Go to VAST2 > Settings > License > Export license.

1-4. Click the Export license button and select your Windows desktop as the destination folder. A VAST2 license folder will display on the desktop, zip the folder and send the request file back to your sales representative, distributor, or VIVOTEK.

The generated MAC list should look like this.

E(F) 編輯(E)	格式(O)	檢視(V)	說明(H)			
2D118F6C9						
re 1 2D118F6C9						
re 2 2D130D08B 2D118F6C9						
re 3 2D13A0741						

You can examine your current license status. Click on Purchased package. The licenses currently in use will appear.

	Purch	nased package ×		
	Name	License (used/total)		
Status Site name	Google map	8/101	Purchased licenses	Advance Package
Lori's CMS			100	Purchased package
-Active Server	GPS receivers		100	Purchased package
	TCP message	0/100		
	POS	1/100		
	Failover	5/101		
	Data Magnet	0/101		

1-5. Once you acquired the MAC licenses from VIVOTEK, click Import MAC license button. You will enter the import page. Use the Add button and locate your license files.

To use the MAC license import function, both the CMS and its substation servers should both be running VAST revision 2.6 or above.

add a MAC license, then select sites to import your MAC license.		0.0	Purchased licenses
	Status	Site name	Purchased licenses
	- 10 - 10 - 10 - 10 - 10 - 10 - 10 - 10	-Active Server	100
Drop a MAC license here			
or click add button			
Add			

1-6. Select the license file.

🔽 開啟苦悩					
🕢 🕞 - 🕌 🕨 電磁 🖡 Ad	cer (C:) , Program Files (x86) , VIVOT	EKInc • VAST • Client • VAST2 •	- 4- 援尋 VAST2 ₽		
組合管理 ▼ 新増資料夾	l		E • 🗌 🛛	nagement	
	 記() () <	 (学会互用) 2019/99/上午10. 	攝於更預要的傷窩 ·	Status Site name Lori's CMS Active Server	Purchased licenses 100 100
横案名	稿(N):		▼ license file (*.lic) ▼	· · · · · · · · · · · · · · · · · · ·	
			開飯芸描(O) 取消	I	
		or click add button	Import		
		Add			
			+		

1-7. The selected file appears on screen.

port MAC license		
a MAC license, then select sites to import your MAC licen	ie.	
	Status Site name	Purchased licens
	CMS	0
	-Store 1	0
	Store 2	0
MacLicense.lic	-Store 3	0

1-8. Select the target server sites to import the license file. When done, click the Import button.

MAC licenses are not bundled with server hardware. You can import licenses from the CMS server to one or multiple virtual machines running the VAST software.

		Sta	tus Site name	Purchased licens
			CMS	0
			-Store 1	0
			-Store 2	0
MacLicense.lic	Import		-Store 3	0

1-9. Select the virtual machines (sites) running the VAST server to import the license file. When done, click the Import button.

Add a MAC license, then select sites to import your			
		Status Site name	Purchased licens
		CMS	0
		-Store 1	0
		-Store 2	0
MacLicense.lic	Impor	-Store 3	0

1-10. When done, the MAC licenses display on the license page as shown below.

🔊 Settings			System manage	ment			
License							
Cicense (
SMTP			Export license Import li				
tit.			Export license and update it in the	i online license management sys	tem		
references							
	Sta	Site name	# VIVOTEK cameras	# Onvif cameras	Purchased I	Advance Pa	
lback and bugs		CMS	1	0	0	Purchased packa	
		-Store 1	1	0	0	Purchased packa	
		-Store 2	1 (MAC license excluder)	0 (MAC license excluded)	MAC license	Purchased packa	
		-Store 3	0 (MAC license excluded)	0 (MAC license excluded)	MAC license	Purchased packa	
		-Store 3		0 (MAC license excluded)	MAClicense	Purchased packa	
		-Store 3 Total (MAC license excluded)		0 (MAC license excluded)	MAC.license	Purchased packa	

Reminders for VAST Software License

Limitations:

- The Batch import/export function applies when a managing VAST server needs to collect and update the licensing information from subordinate VAST substations and itself. An enterprise may have a central management server and several VAST instances running in branch offices. In that case, the substations will be listed on the device list, and may not be displayed on a hierarchical structure.
- 2. The batch download/import function only takes effect on a VAST instance running on server, not on the Linux-based NVR.
- 3. The trial channels on VAST substations will not be available for use on a managing VAST server (one that manages multiple substations).
- 4. If you access a VAST deployment via a web console, the license related information will not be available.
- 5. In this revision, an identical software license applies to both VIVOTEK and other-brand cameras (ONVIF). You do not need to activate two different kinds of software licenses.
- 6. The Batch export update of the current license profile is supported.
- 7. If the VAST server is removed and then re-installed, the number of licensed channels remains intact.
- 8. If users plan to integrate the software licenses from previous dongle licenses, problems may occur if users changed the exported license file name.

Chapter 4 Settings: 4-1. Settings > System > Preferences

The Preferences page for VAST client and Station sides allows you to configure the following:

Client Setting:

- 1. Select the UI text language.
- 2. Configure a default destination for exporting video, snapshots, or configuration backups. The default is "C:\Users\Public\Documents\VIVOTEK Inc\VAST\Downloads". You can change the media format via the checkboxes.
- 3. Select the format for the snapshot as either JPG or PNG.
- 4. You can select the length of the Alarm-triggered videos by specifying pre- and postalarm recordings.
- 5. You can designate the VAST client interface to automatically start once the client computer is started.

VAST2	\$	+ CPU 6% MIM 69% 🏭 🌲	\$ - 16 ×			
🔊 Settings		System management				
Cient Cient Station Samp Preferences Feedback and bugs		Language Export Location C:/Users/Public/Documents/ Snapshot format O JPG PNS Additional video before alarm trigger 1 mins (1-10) Additional video after alarm trigger 5 mins (1-60)				
		On startup Start application on system startup Open set of pages Screen display 2 1 View View 2 View 2				

5. The default Live view, which may span across multiple monitor screens and display Live view, Tour, Dashboard, E-Map, or Alarm prompts. The precondition is that you should configure one or many views before making the Startup configuration.

Below is a server/client with dual monitors, you can select one view to be displayed on one monitor, or place an E-Map on another. Up to 8 monitors can be configured.

Click the Apply button for the configuration to take effect.

On startup							
Start application or	system startup						
Open set of pages							
Screen display		Screen 1	View	٣	Select one view	Ŧ	
1	2	Screen 2	Emap	*	Select one map	*	
		0					

Station Setting:

1. **Display Watermark over video** - Administrators can select to display watermarks on the video feeds of the VAST clients. The opacity and display frequency can be adjusted.

Encrypted watermark for authentication:

To ensure your video is authentic and has not forgerized, adding an encrypted watermark on the data stream can be achieved with a customized password. You can use the Standalone Player to verify which frames in the video footage have been tampered with.

If enabled, the following will be displayed: camera name + substation name + VAST2 user name + user computer current time. The purpose of watermark is to preserve evidence if the video screen is recorded using cell phones or other devices.

Station Setting:

2. **Digital watermark** - To prevent forgery of recorded or exported video clips, and to prove the validity of surveillance evidence, digital watermark can be appened to recorded video.

Note that only non-administrator users will see watermarks.

To enable text watermark, use the slide button. Use the Preview function to tune the text opacity and text frequency display on screen.

að Settings	s	System man	agement
0	Client		Watermark preview X
License SMTP	Station	Display watermark over video Watermark will be displayed only for non-admin users. Administrations will not see them. Preview	Station Camera admin 20200803 16:35:33
t¥t Preferences		Digital watermark Watermark Digital watermark Di	Station Camera admin 20200803 16:35:33
Feedback and bugs		Alarm Reserve time 60 days(1~365)	Station Camera admin 20200803 16:35:33
		Log Log level Normal ▼ Reserve time 60 days(1~365)	Text opacity 100% 50% Text frequency 1 8 Apply Cancel

To enable Digital watermark, enter a password that is at least 16 characters long. Once a valid password is available, you can click the Apply button to preserve your setting.

🔊 Settings		System management
C License SMTP	Client Station	Display watermark over video Watermark will be displayed only for non-admin users. Administrators will not see them. Preview
†∔† Preferences E		Digital watermark Watermark Ution (16-64 characters, letters and numbers only)
Feedback and bugs		Alarm Reserve time 60 days(1~365)
		Log level Normal Reserve time 60 days(1~365)
		Bookmark

When you export a video clip, a StandalonePlayer is generated with the exported files.

檔案 常用 共用 檢視	管理				
← → × ↑ <mark>-</mark> → 本機 → Ace	r(C:) → Us	ers > Public > Documents > VI	/OTEK Inc > VAST > Download	ds > CC9381-HV	_20200803_16552
		名稱 ^	修改日期	類型	大小
📌 快速存取		DISC_001	2020/8/3 下午 04	檔案咨料本	
三. 桌面	*	layout.json	2020/8/3 下午 04		1 KE
🕂 下載	*	Standalone	2020/8/3 下午 04		1 KE
2 文件	А.	StandalonePlayer	2020/7/31 下午 0	應用程式	82,733 KE
■ 圖片	*				
UX-ERICLU-NB	*				
Links					
Links			99% Extracting	×	
SmartVCA_Milestone_guide_	VVTK_rev1		5570 Extracting	~	
新増資料夾 (2)					
😞 Creative Cloud Files				Cancel	
🗦 Dropbox Dropbox				Januar	
OneDrive					

Right-click on the StandalonePlayer screen to display the "Verify watermark" function.

			A.		
	igital zoom napshot	Ctrl+Shift+Z Ctrl+Shift+C	. 1		
D	isplay informa erify waterma	ation	>	Show display in	
7.0	- /			Edit display inf	

	Verify watermark	×
Enter password		Verify
Verification status		
Ο	0	0
Frame matched	Frame not matched	Frame without
Frame matched	Frame not matched	watermark

The Verify screen will display. Enter the pre-configured password. Click Verify.

The below result shows that the video is authentic and has not been forgerized.

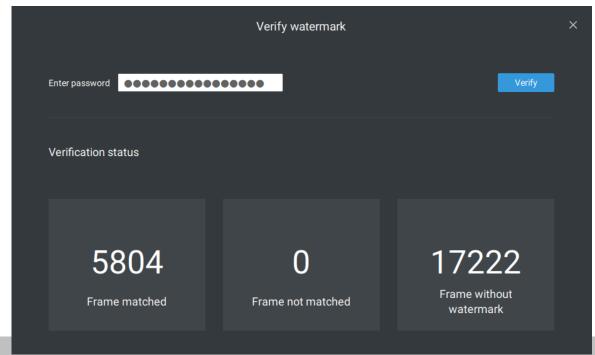
Frame matched: Your video was exported with the digital password, and you entered the correct password.

Frame not matched: Your video was exported with the digital password, and you entered the incorrect password.

Frame without watermark: a. If your video wasn't exported with the digital password.

b. If your video was exported with the digital password, and your video has been tampered.

If the numbers in the "Frame not matched" or "Frame without watermark" are not zero, it means your video is probably not correct.



- 3. **Alarm** Reservation time: Configure the preservation time of the alarms and logs. Note that some alarms can be triggered with recorded videos. Configuring a preservation time can help reduce the use of storage space on server.
- 4. Log: Use the menu to configure the preservation time of the Major, Normal, or Minor logs.
- 5. **Bookmark**: Configure the days of preservation for bookmarks.
- 6. **Data magnet**: Configure the days of preservation for data related to Data Magnet.
- 7. Trend Micro events: Configure the days of preservation for events related to cyber security.
- 8. **Database**: Configure the destination of the database folder. The database contains information for system log, alarms, Bookmarks, data magnet, VCA reports, POS transaction data, snapshots, and Trend Micro IoT security information.

4-2. Settings > Device > Cameras

In addition to the add device process during the initial setup, you can add more cameras or arrange the device list in Settings > Cameras.

Below are the locations of the functions for adding devices to the VAST server.

Settings	(Camera management
	Start Scanning	Add 4 device(s)
Cameras	C Search device(s) Edit device list & Logical folders	Q. IP, MAC, Port, Model, Brand(onvif/vvtk) Authorize + Import CSV
Recording options Sites	✓ VMS_Station ✓ Site1 ✓ Streft ✓ System ✓ System ✓ VMS_Station ✓ VMS_Station ✓ VMS_Station ✓ VMS_Station ✓ VMS_Station ✓ CD8371-HIVF2 ✓ FD8177-H	Status IP - MAC Port Model Brand Status 192.168.6.107 00-02-01-20-1A-BC 80 ProCam v1.0 192.168.6.151 00-02-01-4C-CC-88 80 IP8138-W 192.168.6.170 00-02-01-4E-58-59 80 IB9381-EHT Password protected 38-64-39 80 KX:NTV150 Click to select or deselect Electron deselect Electron deselect
I/O I/O Box	 * "custom_modelname" * "custom_modelname" CD8371-HNVF2 DCS-5615 FD8177-H 	Sync time w/ VAST - or - Sync w/ another NTP server Synchronize camera time with system

Note that you must know the credentials for password-protected cameras. You will not be allowed to enlist cameras that come with unknown credentials.

For cameras outside the local network, you can manually enter its IP address, or use a preconfigured device list to automatically introduce new devices.

If all devices come with the same credentials, you can select these devices and click Authorize to enter the credentials.

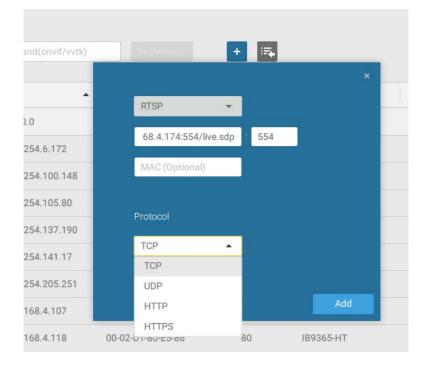
Retrieve RTSP streaming on specific port: The default port for RTSP streaming is 554. If you want to change this port, please check this item and fill in a desired port number.

Streaming URL

This is an optional feature. You can enter a camera's IP address to add a camera's RTSP streaming for live view and recording, and playback.

To insert a camera using the URL-like command,

1. Select the camera Brand as "RTSP."



- 2. Enter the camera's IP address.
- 3. Enter the camera's MAC address as printed on the camera label, or one found by the Shepherd utility.
- 4. Enter "554" in the Configuration port.
- 5. Enter "live.sdp" in the URL field, as this is part of the original RTSP streaming command: "rtsp://172.18.204.58:554/live.sdp". If streaming stream #2, enter live2.sdp.
- 6. Select a preferred protocol.

Note that the free 32 channel licenses does not apply when inserting a camera using the URL command. Only the live view, recording, and playback functions are supported if thus connected. All other functions are not supported, such as auto streaming size or changing to another video stream. Neither are camera DI/DO supported.

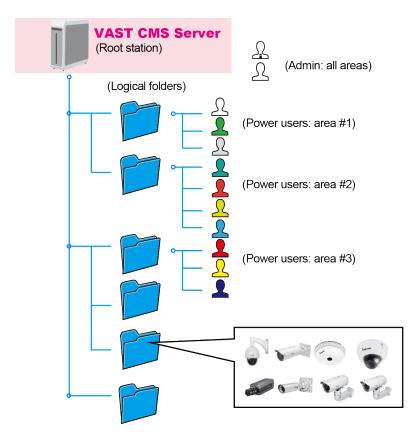
6. For administrators who need to synchronize device time with a NTP server, he can deselect the "Synchronize camera time with system" checkbox.

When adding cameras via ONVIP or RTSP protocol, you can select to synchronize its time setting with your VAST server or to keep the camera setting. The default is using the camera time setting.

VAST2	• • • •			
🔊 Settings			Device	emanagement
Cameras Cameras Sites POS D/DO devices Dot devices Cameras	 Constraint of the second sec	Basic Video Image Motion detection PTZ Settings Multicast €€	Camera name IP Port Brand Time source Protocol User name Password	QNV-7010R 192.168.4.127 80 ONVIF From camera • TCP • admin
VAST2	(10)		Device ma	nagement
Cameras Cameras Sites POS I/O D/DO devices D/DO devices	 ✓ Search devices ✓ Search devices ✓ ✓ VMS_Station_PMtest ✓ MD9541P ✓ FD8365-HTV-v2 ✓ B9367-EH ✓ QNV-7010R → SC8131 ÷ ÷ 	Video Image Motion detection PTZ Settings Multicast	Port 80 Brand ONVIF Time source From Protocol TCP User name admin	68.4.127 server •

4-3. Logical Folders

The Logical Folders allow you to re-define the logical relationships between the real-world deployment and the physical devices (cameras). For example, according to your deployments, you can designate several cameras to be listed under a logical sub-directory named as "Building A," and the other cameras into "Building B." In this way, you can re-arrange your cameras and devices on a tree view that is geographically more accurate.



To create logical folders,

- 1. On the Settings > Cameras page, click the Edit 🖉 button.
- 2. Click on the Add a folder button.
- 3. Enter a name for the folder, e.g., 1st floor, 2nd floor,... according to your needs as shown below.
- 4. Repeat the process to create more folders.
- 5. Make sure you enlisted all cameras in your deployment. You can start moving cameras to specific folders. Click on the Move Selected Items button.

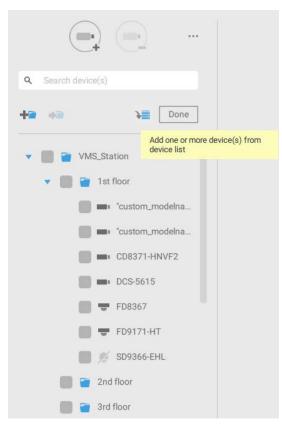
VIVOTEK - A Leading Provider of Multimedia Communication Solutions

Settings		
	•	 Search device(s) +a →a Done
Cameras	Q Sy device(s) +2 →2 Done	■ — 60007.11112
Recording options	Add a folder	"custom_modelname"
Sites	2nd floor	 "custom_modelname" CD8371-HNVF2 DCS-5615
POS	VMS_Station VMS_Station VMS_Station CD8371-HNVF2	✓ ₱ FD8177-H ✓ D8367
I/O I/O Box	FD8177-H	 ✓ ➡ FD9171-HT ■ ➡ FE9182-H

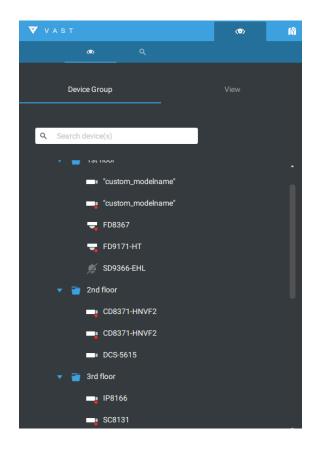
6. Select a logical folder to move the devices to. The selected devices will be listed under the logical folder you selected. Repeat the process to move cameras to each logical folder.

Q Search device(s)	Q. Search device(s)
• Done	Image: Height of the second secon
 VMS_Station 1st floor 	 custom_modelna custom_modelna CD8371-HNVF2
2nd floor3rd floor	 DCS-5615 FD8367
VMS_Station	 FD9171-HT 2nd floor
VMS_Station	3rd floor
	🔻 📗 👕 VMS_Station

You can also use the add device button to select devices from the list and move them to a specific folder.



Return to live view, and you can see the configuration change takes effect.



4-4. Settings > Recording > Recording Options

Click Settings > Recording options. The Recording options window will prompt.

You can configure recording schedules or select the storage options, including the configuration of an external NAS storage.

VAST2	\$	18	1			🏢 🌲 🏟 – 🖻 ×
🔬 Settings				Recording options		
Recording options	 /MS_Station			Archive name DefaultGroup Site VMS_Station 190.79 GB available of 916.15 GB Storage + New storage	1	Recycle Options
Backup Failover				D.vrecording		
				2 Cameras Select cameras	e	Seamless recording
				All cameras	•	
				SD9361-EHL 192.168.4.169 1 • Continu		
						Apply Cancel

Click on any of the options on the Schedule panel for a recording option: Continuous recordings, Events only, None, or Customize.

 Submitted
 Submitted
 Fit
 State

 Submitted
 Submitted
 State
 State

 Submitted
 State
 State
 State

 Submitted
 State
 State
 State

 Submitted
 State
 State
 State

You can manually create a recording template using the New template + New template button.

Click and hold down on the time cells, and drag the mouse to include the time span of your preferrence. The minimum selectable unit is half an hour. You can select multiple time spans on the template. Enter a name for the template, and click Add to save your template.

The same configuraion window apply to both the Schedule template and the customize schedule windows.

Make sure a Schedule mode is selected when you leave this configuration step.

4-5. Settings > Recording > Backup

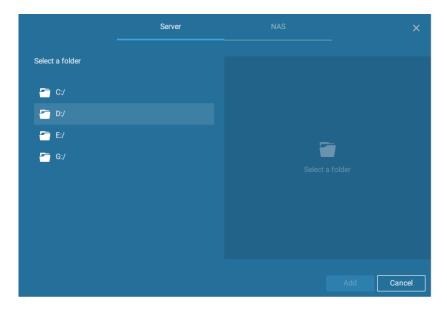
The Backup function allows you to regularly back up the video recordings of one or multiple cameras to local hard disks or a Network Attached Storage device. Currently, the VAST2 server does not support backup to external storage devices such as a storage devices connected via Fibre Channel. VAST supports backup to an external storage attached through a USB 3.0 connection.

Note that the alarms associated with individual cameras will not be backed up.

VAST (D)		4 🕸	- 19 ×
🔊 Settings	Backup		
Recording options	Enable backup		ĺ
Backup	Storage + New storage		
Fallover	Select backup cameras		
	Schedule Not in Working Hours •		
	Options		
	1M 100 M 30		
	Backup from: 2 days ago • Delete old backups if there's not enough storage available	Cancel	

To enable a backup schedule,

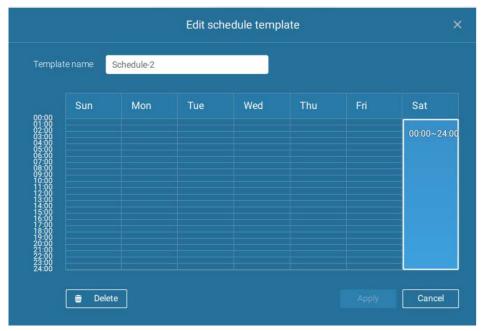
- 1. Enable the backup by selecting the "Enable backup" slide switch.
- 2. Click to add New storage. A configuration window will prompt showing all accessible storage. Click the NAS tab to enable access to a network share.



3. Select the cameras whose videos will be backed up.



4. Select or configure a new schedule template for the backup process to take place. You can select a time when the network load is low, such as the off-office hours, to avoid network congestions.



5. On the Options pane, you can configure an upper bandwidth threshold (in Megabytes) for the backup operation (for all selected cameras/channels).

You can select the extension of time, such as starting from how many days ago, of your backup task. You can select to remove old backups when you run short of storage volume.

Options		
Upload limits:	C Enable	
	1M 100 M 30	
Backup from:	2 days ago 🔹	
💟 Delete old	backups if there's not enough storage available	
		Apply Cancel

Storage

By default, VAST will check there is a D: drive. If not system drive C: will still be defined as the first storage option. Other disk drives in the system, and the default storage volume (configured in the initial setup) will be listed.

You can add a NAS storage's share volume as the additional storage option. Enter the necessary information for access to a network share. Enter and select a NAS path. The share will then be available for video recording.

		×			
Ν	New NAS storage		Selec	ct NAS path	
	192.168.6.117			False_NAS	
	Host			Users	
	User name				
	Password				
	Connect	Cancel		Select	Cancel

Select storage volumes each by a single click.

Click **Ready to use** to continue.

4-6. Settings > Device > Sites

The VAST2 allows a deployment consisting of multiple VAST instances at different sites. A VAST server can be selected as the CMS (Central Management Server) to manage sub-stations in a hierarchical structure.

Each individual VAST station manages its own surveillance deployments. To build a hierarchy, proceed with the following:

- 1. Open the VAST 2 client on a sub-station.
- 2. Enter Settings > Sites.
- 3. Enter a TCP Port number if your network configuration requires a different port.
- 4. Select Allow CMS to access this site.
- 5. Click Change password. This password will be used to authenticate the connection between a CMS VAST server and sub-stations.

VAST	•	• •	CP0 16% MEN 76% 🗮 单 🕸 - Fa 🔹	ж ्रे
🔊 Settings	a.		Site management	
Cameras Cameras Recording options Sites Sites POS I/O I/O Box	Image: Control of the second seco	P	Name VMS_Station State State State State VAST CMS VAST Change password Fir CMS scenestion only	

- 6. Click the Apply button.
- 7. Open the VAST 2 client on the server chosen as the CMS.
- 8. Click the Add sites 💷 button.

9. You can click the Search button if the sub-station is reacheable in a local network, or manually enter the IP address, and password for making the connection.

	Search	
IP/Domain name	1	
Port	3443	SSL only
Add as a red	lundant serve	r

10. Enter the password you configured for the Sites configuration, and then click the Authorize button.

Settings Add 1 sites 🔍 Q Sites MS_Station B Status Name ▲ IP Port Model 192.168.4.169 ND9322P 443 ND9322P 192,168,4,191 443 a ND9322P ND9322P 1/0 C. 4

Click the Apply button for the configuration to take effect.

The sub-stations and its subordinate devices should be immediately listed under the CMS station. You can create separate views to place the sub-stations' cameras.

VAST.	•
0 Q	
Device Group	View
Q. Search device(s)	
 WMS_Station WMS_Station 	
🔻 🍟 VMS_Station	
CD8371-HNVF2	
custom_modelname*	
🔫 FD8177-H	
🛒 FD8377-HV	

When you want to enlist an NVR into your configuration, please remember to enable the access from VAST server in the NVR's Service page.

The connection between VAST and NVR is made via encrypted https.

If the connection port is changed to a non-SSL port, the access from VAST to NVR will fail. For adding the ND series NVR, use port 443.

*v	IV©TEK	•	ጽ 🤹		14:57	43	e admin (Log out)
	Overview		Service por	+			
	Camera		нттр	80			
			HTTPS	443			
	Alarm		RTSP	554			
	System		CMS & iVie	ewer			
	User		Allow ac	cess			
			Port	VAST & iViewer	3454		
	Storage			VAST2 (same as HTTPS)	443		
٢	Network	IP	CMS	Set up password for VAST & VAST2			
	Applications	DDNS		Confirm password			
i	Information	Service		VAST2 remote connection			

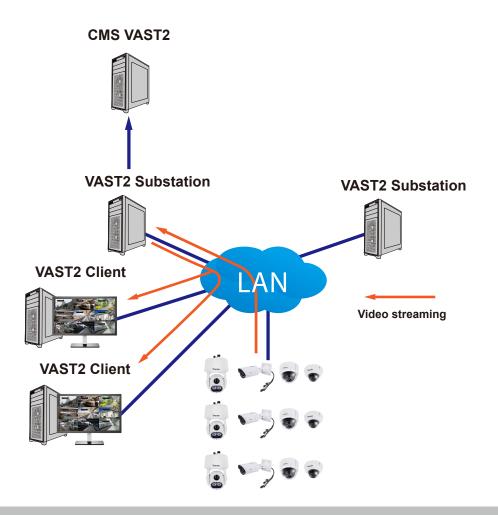
Multicasting

The VAST2 supports multicasting of live streams from server to clients. If multiple VAST2 clients demand live videos from the same camera, multicasting cna help save considerable system resources.

Multicasting should be enabled on a VAST server and also on individual cameras.

There are prerequisites:

- 1. Both the VAST2 server and clients have to be revision 2.7 or above. If any of them is running revisions before 2.7, client connections will crash.
- 2. Multicasting is not supported under the following conditions:
- * A CMS local client can only access the live stream from the cameras managed by the CMS server using unicast connections.
- * If the need arises for access to cameras managed by VAST sub-stations, the multicasting configuration should take place on the sub-stations instead of on the CMS server.



* If the streaming connection for a sub-station is configured as **CMS Relay**, you should configure the multicasting settings on the CMS server.

VAST2	@ 1	+ cru 11%, wax 23% 🗮 🌲 🛊 - a x
🔊 Settings		System management
Conse SMP HH Preferences	Chert	Consistent of spage Image: Constraining connection Image: Constraining connection

- * To enable multicasting, your network infrastructure must support the IP multicasting standard IGMP (Internet Group Management Protocol). Your server and clients should be on the the same network segment.
- * Multicasting is only possible for live streams, not applicable to the recorded video or audio.
- * Multicast streams are not encrypted, even if the the recording server uses encryption.
- * The IPv4 multicast address range is: 224.0.0.0 to 239.255.255.255.
- * A layer 2 network switch that supports IGMP is required in the configuration.

To enable Multicasting on a VAST server:

- 1. Enter Settings > Device > Sites.
- 2. Single-click to select a server for which you want to enable the Multicasting.
- 3. Click the checkbox to enable the configuration and enter the multicast address.
- 4. Click the **Apply** button.

Starting the Multicasting service will restart the VAST server.

VAST2	۵	\$	+			сеџ 9% мем 24% I 🏢 🐥	🕸 – 16 ×
🔊 Settings					Device management		
Cameras Cameras Sises U/O DUOO devices Cation magnet Cata magnet External devices	1	And devices orf's CMS (192 ND8212W NV9411P Sydney Off Sydney Off VMS_Static	ce	Model CMS Multicas	le multicasting of live streams from servers to clients		Cancel

To enable Multicasting on a camera:

- 1. Enter Settings > Device > Cameras.
- 2. Single-click to select a camera for which you want to enable the Multicasting.
- 3. Click to select the Multicast tab.
- 4. Click the Multicasting slide button.
- 5. Click the **Apply** button.

VAST2	o (\$ +		CPU 14% MEM 23% 🗰 🌲 🏟	- 6 ×
🔊 Settings	a)	Device management		
Cameras Sites Sites POS U/O devices DI/D devices DI/D devices External devices	 entropy <	Basic Autocasting of live streams from servers to clients ● Yide Autocasting for corresponding server in Sites before turning on Otherwise, it will still remain uncasting. Furthermore, if CMS relay is selected arearing connection, you will have to set up multicast on CMS.	n multicasting.	

4-7. Settings > Device > POS

To connect a POS machine, make sure the POS machine is connected to the local network. Click

on the Add POS 💷 button.

- 1. Enter a device name, such as POS on the 1st floor counter.
- Select the POS brand name. Currently VAST2 supports Lafresh, POSNET, Gulfcoast(POS Gateway).
- 3. Enter the IP address assigned to the machine.
- 4. Enter the TCP port number utilized by the POS machine for network connection
- 5. Select a related camera whose video feed will be used to display POS transaction data. This is the camera which covers the customers and cashier.
- 6. Enter specific item name or a total amount exceeding a high threshold, such as using >100 as a threshold. You can enter multiple highlight conditions using the add button below. The highlighted entries will be displayed in bright font colors on screen.

VAST2		\$			CPU	Add a PO	s		
🔊 Settings			POS m	nanagemen	t				
						Device name			
						Brand	LaFresh	•	
_	Q Search	devices				IP			
Cameras						Port			
Sites						Related came	ra FE9381-EHSV	•	
E						Highlight text	of transaction details on L	ive	
POS						Press "Enter" fo	r each logword		
I/O						All	• e g >100, blue per		
DI/DO devices						All	▼ e.g. >100, blue per		0
C.						All	• e.g >100, blue pen		0
Data magnet						All	_		
4						Item name			
External devices						Total			

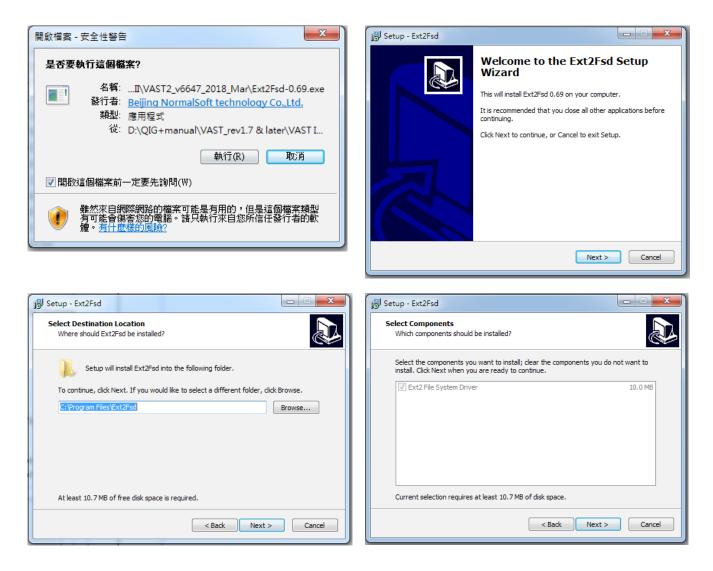
4-8. Settings > Device > Local DB

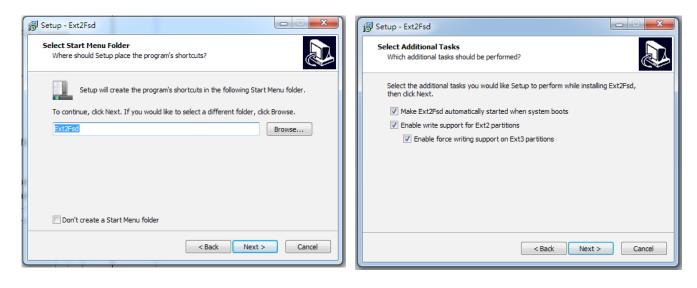
Since some of VIVOTEK's NVRs runs on Linux, you have to install the Ext2 File System Driver for Windows to access the recording files from a NVR hard disk.

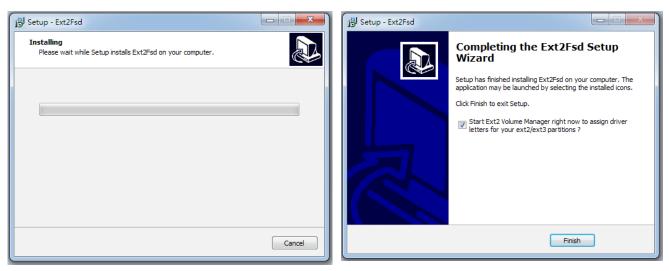
The file system driver can be found here: https://sourceforge.net/projects/ext2fsd/?source=typ_

redirect

Run and install the Ext2fsd-0.xx.exe. Follow the onscreen instructions to complete the installation.

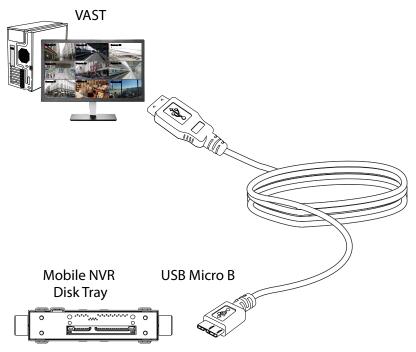






Volume	Туре	File system	Total size	Used size	Codepage	Physical object
\$	Basic	RAW	128 MB	128 MB		\Device\HarddiskVolume1
\$	Basic	FAT32	99 MB	99 MB		\Device\HarddiskVolume2
🧼 (C:)	Basic	NTFS	916 GB	916 GB		\Device\HarddiskVolume3
\$	Basic	NTFS	499 MB	499 MB		\Device\HarddiskVolume4
🧼 (D:)	Basic	NTFS	916 GB	916 GB		\Device\HarddiskVolume5
\$	Basic	NTFS	29 GB	29 GB		\Device\HarddiskVolume8
\$	Basic	RAW	128 MB	128 MB		\Device\HarddiskVolume7
ം ശ	Basic	NTES	1862 GB	1862 GB		\Device\HarddiskVolume8
•			111			4
	Туре	File system	Total size	Used size	Codepage	Partition type
DISK 0						
	Basic	RAW	128 MB	128 MB		GPT
	Basic	FAT32	99 MB	99 MB		GPT
(C:)	Basic	NTFS	916 GB	916 GB		GPT
	Basic	NTFS	499 MB	499 MB		GPT
(D:)	Basic	NTFS	916 GB	916 GB		GPT
	Basic	NTFS	29 GB	29 GB		GPT
DIOK 1						
DISK 1		BAW	128 MB	128 MB		Microsoft reserved partiti
	Basic					

- 1. Remove the disk tray box from a mobile NVR.
- 2. Connect the disk tray box to your VAST server using a USB 3.0 type A to Micro B cable.



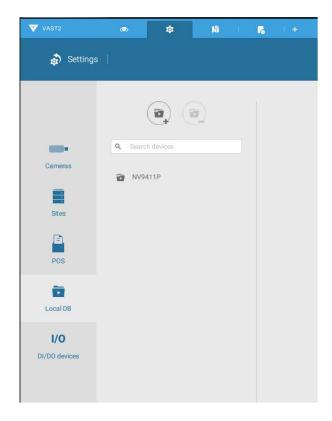
- 3. From VAST, enter **Settings > Device > Locabl DB**.
- 4. There are 3 import types:
 - 1. **NVR disk**: the drive tray box removed from a mobile NVR.

2. **NVR backup**: the recorded videos exported from an NVR using a USB thumb disk or portable drive.

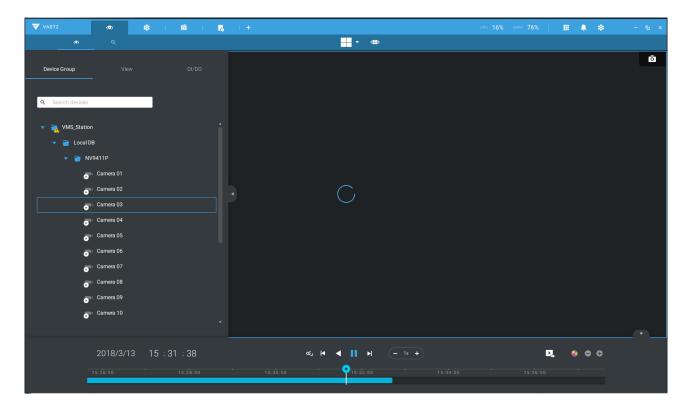
3. **VAST backup**: scheduled backup from the local machine. They include: VAST backups from previous software releases, and scheduled backups.

VAST2	\$ +		сни 13% мем 75% 🏭 🌲 🏟 — На 🗙
🔊 Settings		Recording management	
Recording options Backup Failover Local DB	Image: Constraint of the	● OneDrive 各時 #2日時 ■ sedio 2019/6/5 Fre02_ ■ 30 % # audio 2019/6/5 Fre02_ ■ 30 % # Imagiformatis 2019/6/17 Fre0_ ■ Trit Imagiformatis 2019/6/17 Fre0_ ■ 27 # platforms 2019/6/17 Fre0_ ■ ## # 2019/6/17 Fre0_ ■ ## QfCharts 2019/6/17 Fre0_ ■ ## QfCharts 2019/6/17 Fre0_ ■ Data (D) QfOpulk 2019/6/17 Fre0_	集整茶料 集整茶料 電整茶料 電整茶料 集整茶料 集整茶料 電整茶料 電整茶料

- 5. Taking a mobile NVR's disk drive as an example, click the 🔎 Source select button to locate the disk drive.
- 6. The NVR will be mounted as a local DB.



7. A Local DB sub-tree will be listed under your server, and you can view the existing recordings on the NVR's disk drive.



4-9. Settings > System > SMTP

Configure a mail server via which the system alarms or notifications can be delivered to a receiver.

Enter the Settings page, select SMTP. Click on the Add SMTP button.

Enter your mail server's domain name or IP address. Enter credentials for access to the mail service.

If SSL encrypted transmission is preferred, select its checkbox.

Click Add to complete the configuration.

4-10. Settings > IO Box and Related Configuration

Please refer to page 175 for information.

4-11. Settings > User Management

The User Add & Delete page allows you to create users with the permissions for different operational capabilities.

To specify the authorized privileges, select Customize in the Role menu, then select the Permissions and/or the Accessible devices tabbed menus.

🔊 Settings		Add & Delete
Can Search users	New user	
admin admin vivotek.tw\eric.lu	User name	operator AD account
	Password Confirm password	•••••
	Role	Administrator Administrator Customize
		Add Cancel

Use the Customize option to limit the authorized actions of a user.

In the Permissions tab, click the expand button 🕨 to unfold the Operation and Configuration menus. Select or deselect the checkboxes to

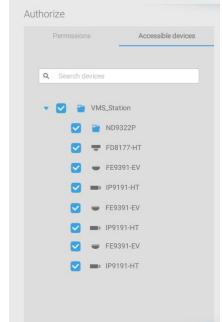
configure the user privileges. For example, you may not want

a user to operate Alarm and E-Map. If so,

deselect these checkboxes.



In the Accessible devices tab, click to select the cameras that a user can access. Some users may only need to access specific devices.



When done with the privilege settings, click Add to create a new user.

The new users will be listed under the Administrator's icon. Repeat the process to create more users.

Add a New User Account - Windows AD Account

In an established, enterprise network environment, the support for Windows AD (Active Directory) infrastructure enables ease of integration using the credentials of existing users. Using the same AD authentication methodologies, you can configure the clients or users in an established network to access the VAST server configuration.

Note the following with Windows AD support:

- 1. If you install VAST server on a Windows XP machine with Postqre SQL server, the login using a Windows AD account will not work.
- 2. The VAST server must reside in a domain managed by the AD server.
- 3. This function does not support the environment that spans across multiple AD domains.
- 4. A user account hosted by an AD server cannot be modified in VAST.
- 5. A User Group and its members configured in AD cannot be managed in VAST.
- 6. You cannot add an account having the same name as one you used to log in VAST.
- 7. There are 3 types of account for VAST: VIVOTEK account, AD single user, AD group.

To add an existing AD user,

1. Select the AD account checkbox.

🔻 VAST 💿	\$	
🔊 Settings	Add & Delete	
 e Search users e admin e vivotek.tw\eric.lu 	New user User name Vivotek.tw/frank.chang Value AD account AD account AD account Confirm password Role Administrator An administrator has all permissions and is allowed to access all devices	Cancel

2. Click the Search ^Q button.

3. Enter a user name or group name to search, e.g., Frank. Click OK when done.

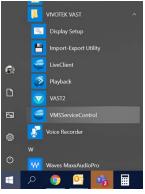
ollowing object na		ound	···
amples): Multiple	e Names Fo	Check Nam K Cance	
Multiple	e Names Fo	Check Nam K Cance	ies d
Multiple	e Names Fo	Check Nam K Cance	ies d
Multiple	e Names Fo	K Cance	
ollowing object na	e Names Fo	K Cance	
ollowing object na	e Names Fo	ound	
ollowing object na	e Names Fo	ound	
ollowing object na	e Names Fo	ound	
ollowing object na	ame: "admin". S		
ollowing object na	ame: "admin". S		
name, click Cano			
•	lail Address	Description	In Folder
rator rators		Built-in account f	ericthegreat 123 ericthegreat 123

- 4. Enter the password twice for the AD user.
- 5. Select the privilege role for the user, configure his/her privilege settings as described above and then click Add.

Appendix A: VAST Service Control Tool

VAST service control tool is a tool for server control and for user to be aware of the VAST Server status. It starts up as Windows OS startup.

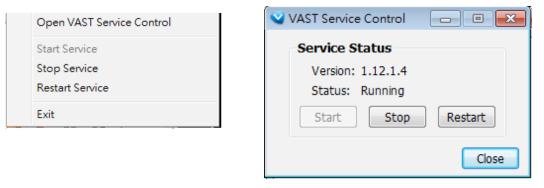
Under Microsoft Windows, choose "Start > VIVOTEK Inc VAST > VMServiceControl."



You may also find it in the system tray icon of the tool bar, which indicates that the service is running:

It shows a disconnection icon when the service is stopped: 🖤

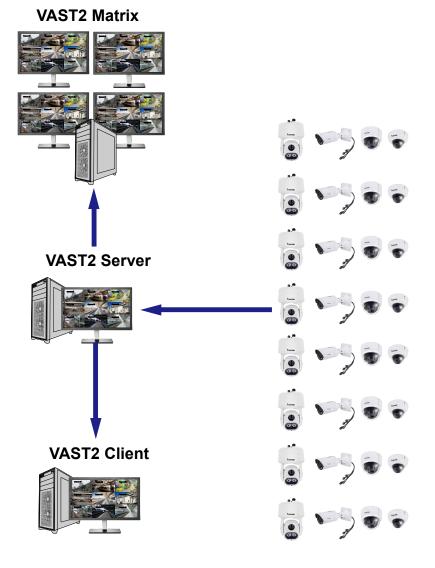
A menu for the service control tool will pop up when you **right-click** on the icon:



Here you can manually start, stop and restart the service.

Appendix B: Matrix

The virtual matrix feature enables the display of any cameras on any monitors in an IP surveillance network. Combinations of live or playback streams can be displayed simultaneously. In addition of pre-configured live views, E-maps, Google maps, and Alarm panes can all be placed on a remote matrix. Users gain realtime awareness of scenes and access to past events.



Prerequisites:

- 1. One VAST2 server and another computer running the Matrix client utility.
- 2. The first 2 digits of software revision numbers of VAST server and Matrix client must be the same: e.g., 2.3.x.x and 2.3.x.x.
- 3. Sufficient network bandwidth among network cameras, VAST servers, and Matrix clients.

Configuration procedure:

1. Install the Matrix client utility on a computer equipped with multiple monitors. Follow the onscreen instructions to install the utility.

VIVOTEK Matrix Installation	VIVOTEK Matrix Installation
Choose the folder in which to install the Matrix.	Read this license agreement carefully before Vivionia installing. v2.10.223
Setup will install Matrix in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.	End-User License Agreement PLEASE READ CAREFULLY: This End-User License Agreement ('EULA') is a legal agreement between VIVOTEK Inc. ('VIVOTEK') as
Installation folder C:\Program Files (x86)\VIVOTEK Inc\Matrix Browse	licensor, and you, as licensee, for the VIVOTEK software that accompanies this EULA, which includes remote management software and other applicable software (the "Software"). YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE OR CLICKING THE BUTTON MARKED 1 AGREE" OR "YES" BELOW. IF YOU DO NOT AGREE.
Cancel < Back Next >	Cancel I Agree
VIVOTEK Matrix Installation	VIVOTEK Matrix Installation
Installing	Тупуотак
<u>v2.1.0.223</u>	<u>v2.1.0.22</u>
Installing Matrix client	✓
30%	Install successfully
Cancel Retry	Cancel Done

2. On the VAST server, create a user account for the Matrix client. Depending on the operation on the client computer, assign the client user with adequate operation privileges.

VAST2	۲	\$ +	
🔊 Settings	1		Add & Delete
 Search users Search users admin Matrix_clie 	nt		New user User name Image: AD account Password Confirm password Role Administrator An administrator An administrator has all permissions and is allowed to access all devices

3. Open the Matrix utility, log in to the VAST server address, using the Matrix client account credentials.

Matrix Client		
192.168.5.121	3443	
Matrix_client		
Password		
AD account		
Auto login		

4. From the VAST server, open the Settings > Matrix Management window.

VAST2	۲	\$	+				
		P .				((🌒))	1000
		Device	è	Recording	g	Alarm	User
		Cameras		Recording options		Add & Delete	Add & Delete
		Sites		Backup			
		POS		Failover			
		Local DB					
		DI/DO devices					
		Data magnet					
		Matrix	¢.				
		Matrix managen	ent				

5. Enter the name of your Matrix client, e.g., Matrix_client in the search pane of the Matrix Management window. Note that the Matrix client must have logged in to establish the connection before the VAST server can find it (as previously described).

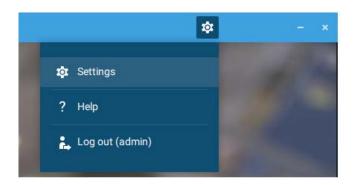
VAST2 💿	\$	+
🔊 Settings		Matrix management
Q Search users or computers		All
	\nearrow	View E-Map Alarm
		■E. ▲ G 単 単 Alarm

Once the VAST server found the Matrix client, the available monitors will be listed. Click and drag the pre-configured Views, Tour, Dashboard, E-maps, or Alarm panel to any of the monitors.

VAST2 💿	🌣 🖂 I +	CPU 8% MEM 29% 🛛 🏭 🌻	– 🗆 ×
🔊 Settings	Matrix mana	agement	
Q Search users or con ✓ admin 	All Drag the following feature View Dashboard E-M E-M E-M E-M E-M E-M E-M E-	es to your displays	Reset all
		JL	

7. The views should immediately appear on the Matrix monitors.

8. If you need to log out, move your mouse cursor to the top of the Matrix client screen to end the session.



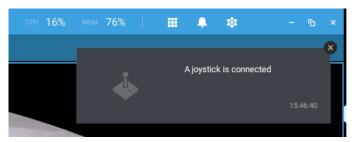
If necessary, change your client settings. Here you can change the displayed language, Export target folder, Start-up option, and the streaming connection options.

	Settings	×
System preference		
	Language English •	
	Export Location C:/Users/Public/Documents/ To Snapshot format O JPG O PNG	
	On startup Start application on system startup	
	Substation streaming connection CMS Relay Direct link	
	- Appelling - Constant	

Appendix C: Joystick Support

Configurable joystick buttons

- 1. Connect the joystick's USB cable between the USB ports on the joystick and a VAST server/ client.
- 2. Once connected, you should be prompted by a connection message.



- 3. Enter Settings > Device > External devices.
- 4. Single-click to select the detected joystick. The configurable buttons will be listed. Click ► to expand the Live, Playback and Common menus.

VAST2	۲	\$	Ļ	1 🖂	- I - G		CPU 12% MEM 34%	I III ♠	¢	
🔊 Settings					External	devices				
Cameras Cameras Sites POS I/O DI/DO devices Cameras External devices		3D Joystick Keyb	board		Assign Select on Action	joystick buttons e of the actions belo is e Home Pan Stop Patrol Patrol Preset ESC	S w and press a Joystick button to a Buttons Button 3 Button 3 Button 1 Button 2 Button 7 Button 7 Button 7 Button 23 Button 23 Button 25 Button 26	assign to	Cancel	

5. To assign or re-assign a button's function, single-click on the button number besides a

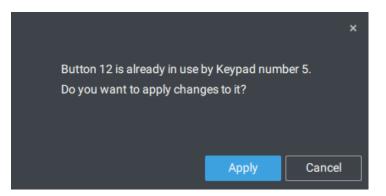
function. Click the Delete 💿 button. The below message will display.

Stop

Press a joystick button

Press a preferred button on your joystick to complete the setting.

If a button conflict occurs, (another function has already been assigned to the same button), the below message will prompt. You can Cancel or click Apply to change the assignment.



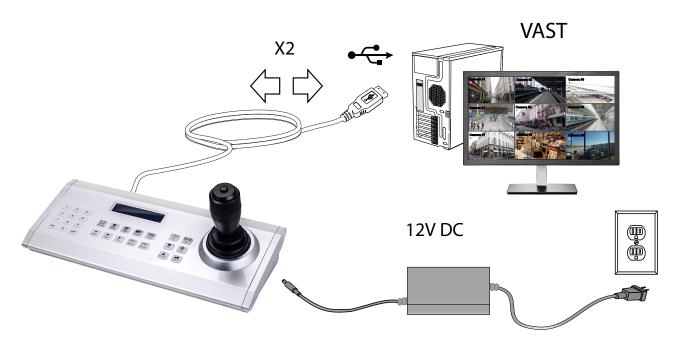
Repeat the above process and click the **Apply** button to preserve your settings.

VIVOTEK's joysticks

The AJ-002 is a USB joystick with HID 3-axis PTZ control, a twist wheel for zoom in/zoom out, and 29 configurable function buttons for use on a VAST server station.

Following are the conditions for making the connection:

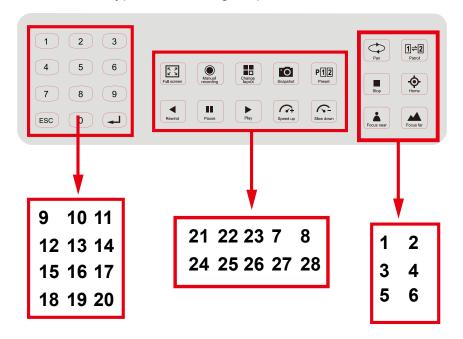
- 1. The joystick can either be powered by a DC 12V adaptor or via the USB. If powered by USB, plug the USB cable twice to the USB port to enable USB power.
- 2. Connect the included USB cable between the USB ports on the joystick and a VAST server.



- 1. Avoid spilling water onto the device. Avoid using this device in a high-moisture environment.
- 2. This device should be operated in the indoor environment.
- 3. When the temperature is lower than -10°C, the LCD panel may not function normally.
- 4. If the included power adapter should be replaced, use a 9-15V/1000mA alternative.
- 5. Avoid impact to the device.
- 6. This product is manufactured to comply with the requirements of the following directives: 89/336/EEC, 92/31/EEC, 93/68/EEC.

KEYPAD DEFINITION

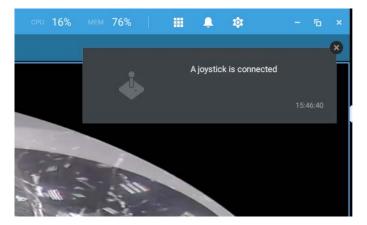
Below is the keypad numbering sequence:



The following keypad functions will be available as the defaults for the joystick.

1	Pan	9	#1	17	#9	25	Pause
2	Patrol	10	#2	18	Cancel/Clear/Esc	26	Play (Playback)
3	Stop	11	#3	19	#0	27	Speed Up
4	Home	12	#4	20	Enter	28	Speed Down
5	Focus Near	13	#5	21	Full Screen		
6	Focus Far	14	#6	22	Manual recording		
7	Snapshot	15	#7	23	Change Layout		
8	Preset	16	#8	24	Rewind		

When a joystick is connected, the VAST server should automatically detect the connection.

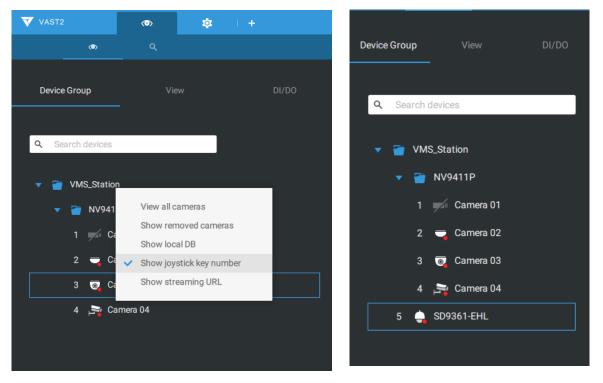


The following controls are available:

- * PTZ control Basic PTZ control: Direction, Home, Zoom in/out, and Focus near/far.
- * Playback control Play, Pause, Stop, Rewind, Speed up and Slow down.
- * View switch Switch to existing View (Users need to create views first).

Left-click to select your server on the device tree, and right-click to display and select the "**Show joystick key number.**" The camera key numbers are determined by the sequence when the cameras were added to the VAST configuration, and cannot be changed. By default, the key numbers are not shown.

Press the key number on the joystick keypad and the Enter key -1, e.g., 5 + -1. The full view of the selected camera will display.



Press the ESC key to leave the full view.

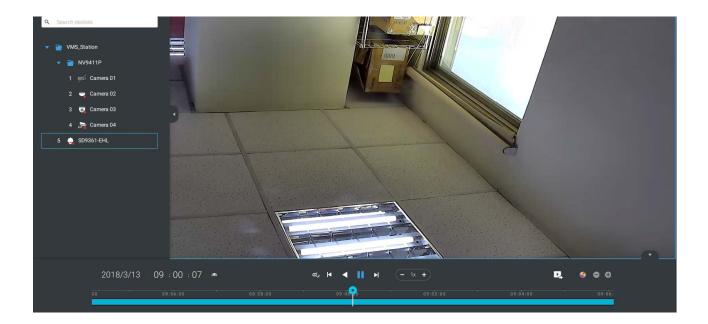
To move to a preset position, press the number key + Preset, and the Enter key - . The number key corresponds to the sequence number for the preset position regardless of the name of the preset.

Note that the RS232/485 terminal connection is currently not supported.

Note that the Manual Recording button is currently not effective.

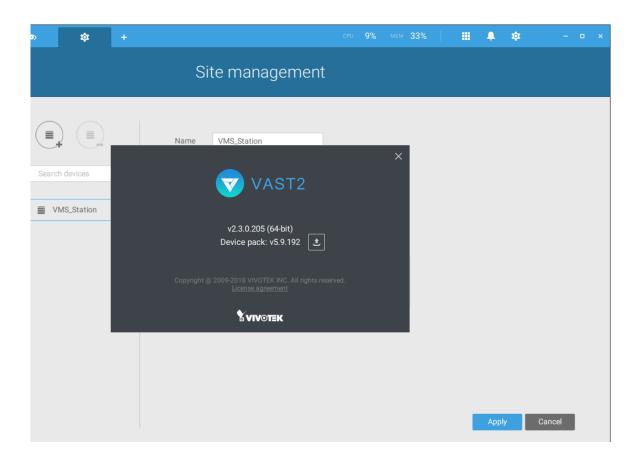
If you have multiple views, press the number key and the Change Layout, and the Enter key to switch to a different view. The number key corresponds to the sequence number for the view you configured regardless of the name of the view (layout).

The Play button toggles the playback window. From here you can trace back the past recordings. You can use speed up, slow down, and rewind buttons here. Once the Playback mode is toggled, the point-in-time defaults to the start of the current hour.



Appendix D: Upload Device Pack

A device pack is contantly updated for the latest profiles of VIVOTEK's new camera/NVR models. If you install new cameras/NVRs to your configuration, you can visit VIVOTEK's website for the latest device pack updates, and upload the pack file to your VAST server. New functional parameters and functions in the new cameras are available through the device pack.



Enter Settings > About to see the upload button.

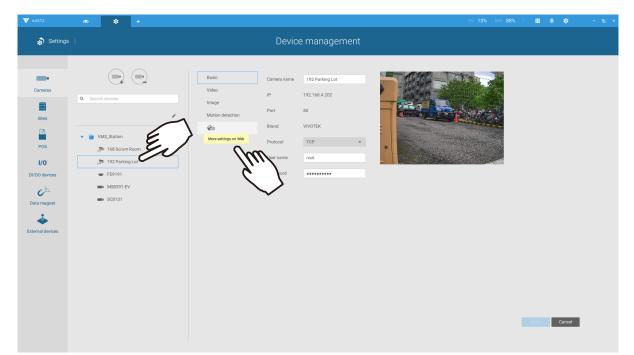
A device pack file looks like the following.

-> -> 🛧 🗖 > Th	is PC > Desktop >	ٽ ~	Search Desktop	
rganize 👻 New folde	r			EE 🕶 🛄
PJM ^	Name	D	ate modified	Туре
VAST 2.3 annour	1.12.7.1	9,	/13/2018 3:36 PM	File folder
ConeDrive	Nr9x81	9,	/17/2018 2:15 PM	File folder
onconte	NR9x82	9/	/17/2018 2:16 PM	File folder
This PC	🍄 PicPick 5.0 Portable BY GDaily	6,	/24/2018 11:10 PM	File folder
3D Objects	VAST 2.3 announcement	9,	/17/2018 2:01 PM	File folder
E Desktop	device_pack-5.9.200.vdp	9/	/17/2018 3:50 PM	VDP File
Documents	Product	9/	/12/2018 2:42 PM	Shortcut
Downloads				
Music				
E Pictures				
Videos				
🚣 Acer (C:) 🗸 🗸	<			
-	ame: device_pack-5.9.200.vdp	~	Device Pack (*.v	(dp)

Appendix E: Using LPR Related Functions w/ Data Magnet

Acquiring data sources from 3rd-party software:

 Select a camera that comes with the LPR (License Plate Recognition) functionality, e.g., IB9387-LPR as shown below. Click "More settings on Web" to open a web console to the camera.



2. On the web console, enter **Configuration > Applications > Package management**. Click on ANPR to open a web console to the license plate recognition software.

		Home	Client settings	Config	uration	Language
	Applications > Package man	agement				
System	Status License					
Media	- Upload package					
Network	Save to SD card Select file	Browse.	Upload			
Security						
РТΖ	Resource status CPU Status:					
Event	Storage status:					
Applications	SD card status: Ready					
Motion detection DI and DO Tampering detection	Memory status: Package list					
Audio detection	Package name	Vendor	Version	Status	License	
Shock detection	O Trend Micro IoT Security	VIVOTEK	1.2b.a1.4.1	Installed	N/A	P 88
Package management	O ANPR	VIVOTEK	2.4.6	ON	N/A	SD 🗯
Recording	Start Stop	Sched	ule			
Local storage						
Version: 0119a						_

3. Click on the **Lists** tab.

	TEK	Live Review Lists LP	R configuration General co	nfiguration	Audit Logs
			Atribute	Value	Last Change
- HEEN	mm		Results:	9984	12:02:26.809 18/09/20
11121		Second Harden	Actions:	15201	12:05:19.732 18/09/201
			Exports:	29	12:00:00.737 17/09/201
			Imports:	1462	18:51:22.681 16/08/201
A. C. Commercial			Triggers received:	0	00:00:00.000 01/01/201
The second second			Frames processed:	29216441	12:06:03.522 18/09/20
	WERE THE REAL PROPERTY OF AND ADDRESS OF ADD	a second	FPS:	2	12:05:26.639 18/09/207
· Distance			SD space free (%):	86	12:06:00.984 18/09/201
•	Calls and the second		Camera space free (%):	66	12:06:00.989 18/09/207
			Last Size (pixels):	37	12:02:28.082 18/09/207
			Last OCR time (millis):	701	12:02:28.075 18/09/207
Show ROI	Show lanes	Calibration pattern	Function mode:	MOTION	12:06:03.525 18/09/201
5L7640 (Taiwan) 99.16% 24.33px 2019-09-18 11:35:19.087	8817L8 (Taiwan) 94.70% 23.17px 2019-09-18 11:50:29.541	ASE5538 (Taiwan) 81.34% 27.29px 2019-09-18 11:57:05.356	1258RK (Taiwan) 87.46% 26.33px 2019-09-18 12:00:56.316		AHX8086 (Taiwan) 80.33% 37.14px 019-09-18 12:02:25.546

4. Select a list whose data will be transmitted to the VAST server.

	VIVOTEK	Live Review	Lists LPR configuration	n General configuration Audi	t Logs	
💌 Lis	st types					
				+ 🛛 Q Search		
ID	Name					
-2	all plates				Edit Delete	
-1	not in list				Edit Delete	
1	BLACKLIST				Edit Delete	
2	WHITELIST				Edit Delete	
▼ Ac	ction for the list: all plates (1)					
				+ Q Search		
ID	Description	Action type	Active			
6	Lori	Socket client	Enabled		Edit Delete	
► Ex	ports for the list: all plates (0)					
				Em.		
▶ lm	ports for the list: all plates (0)					

- 5. 5-1. Find the "Action for the list" pane. Click the "+" Add a row button.
 - 5-2. Enter a short description for the row.
 - 5-3. Select "**Socket client**" as the action type.
 - 5-4. Click to select **Enabled**.
 - 5-5. Click the **Save** button.

A AIAOIEK	Live Review Lists LPR configuration General configuration Au	dit Logs
 List types 		
	Socket dient a Socket dient Q Search	
ID Name	Socket server	
-2 all plates	IO Onvif event	Edit Delete
-1 not in list	FTP Add a row	Edit Delete
1 BLACKLIST	HITP Add a row HILESTONE	Edit Delete
2 WHITELIST	WIEGAND	Edit Delete
 Action for the list: all plates (1) 	Trigger server Select	
	3 + Q Search	
D Description	Action type Active	
5 Lori	Socket client Enabled	Edit Delete
 Exports for the list: a enter a short description Imports for the list: 	on Copyright © 2019 4	

6. Roll down to enter your VAST server's IP address. If necessary, select **XML_IMG** as the file format for your data that will be collected on VAST.

▼ Scheduler		
ACTIVATION SCHEDULER		
0:00 1:00 2:00 3:00 4:00 5:00 6:	00 7:00 8:00 9:00 10:0011:0012:0013:0014:0015:0016:0017:0018:0019:0020:0021:0022:00	23:00
Mon		
Tue		
Wed Thu		
Fri		
Sat		
✓ Save scheduler		
Action Info	?	
Host:	192.168.4.166	
Port:	17000	
Format:	XML • XML_IMG JSON JSON_IMG	?

 Close the web console and return to the VAST Settings > Device management > Data magnet page.

Click the Add button, and click the License Plate Recognition button.

VAST2	\$ \$ +	срч 17% мем 76% 🕴 🗮 Ј
🔊 Settings	3	Device management
Cameras Cameras Sites Dos J/O DI/DO devices Cota magnet	Chip Control of the second sec	Add a data source × Kar License Plate Recognition Third party data source

NOTE

- 1. The License Plate Recognition data source will not be charged with a Data Magnet license fee.
- 2. The VAST server port for License Plate Recognition data source can be customized; It is not limited to 17000.
- 3. If you have more than one VIVOTEK LPR camera, you only need to (and can only) add a License Plate Recognition data source.
- 4. If you add a 3rd-party data source but you name it as "VIVOTEK ANPR", it will be recognized as a VIVOTEK ANPR (License Plate Recognition) data source.
- 5. Different Data sources cannot have the same name.
- 6. Different 3rd-party data sources can share the same server port, but they cannot use the same port the License Plate Recognition is using.

If you need the development document for integrating 3rd-party software, please contact VIVOTEK's technical support.

You can designate how many days the data from the data sources is retained on server in **Settings > System management > Preferences**.

🔊 settings 🔰 System management		
Client Alarm Station Reserve time SMTP Log Log Log Preferences Log Reserve time 60 Bookmark Bookmark Bookmark Bookmark Data magnet		
Reserve time 60 days(1~365)	el	

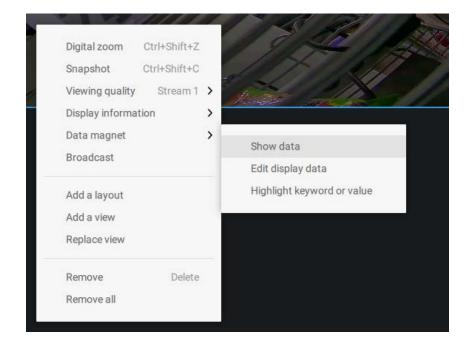
Selecting data display options:

On the VAST live view, right-click on screen to display Data Magnet > Edit display data.
 If Show data is selected, a portion of the view cell will be used to display the captured data.

There are two different ways to show data:

- 1. Right-click: Data Magnet > Show data.
- 2. Right-click: Display information > Edit display information > Data magnet data.

The display options are: with or without Data overlay on screen. If the overlay is not enabled, the data will display on the right pane of the view cell.



The data on the overlay can be configured to automatically disappear after a configurable time, when no new data is received (Hide data after idle _ s).

2. On the Edit pane, select all or manually select multiple display elements.

Edit disp	olay data	×		Edit display data	×
VIVOTEK ANPR All camera char height confidence level country data source data source identity image height image left	Plate number: 93MR = List name: not in list = Timestamp: 2019/08/2 = Country: Taiwan = Camera: IB9387-LPR =		VIVOTEK ANPR image top image width lane name list list name v plate image plate number proc time timestamp	Camera: IB9387-LPR	■ ■

3. Click and drag individual elements to change their top-down positions on the screen. When done, click the **Apply** button.

	Edit display data	×
VIVOTEK ANPR -		
image top image width	93 MR -	
lane name list	List name: not int∰ ≡ Timestamp: 2019/08/2 ≡]
🛃 list name		1
🛃 plate image	Camera: IB9387-LPR 🛛 🔤	J
plate number	Plate number: 93MR 🛛 🗮]
imestamp		
	Apply Cancel	

4. Click **Highlight keyword or value**. You can display information of unusual data, such as the specific numbers or characters of forbidden license plates. When such data is met, the occurrence will be highlighted in a bright yellow color.

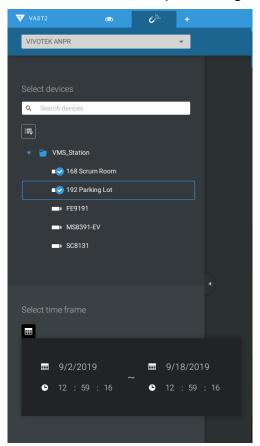
			Highlight keyword or value		>	ĸ
VIVOTEK ANPR	Ŧ					
Press "Enter" for each	keyword					
char height	Ŧ	Text 👻	Key in "=" for text match, "~" for text contain			
identity	•	Text 👻	Key in "=" for text match, "~" for text contain		\odot	
€						
				Apply	Cancel	

Searching for data and linked recordings:

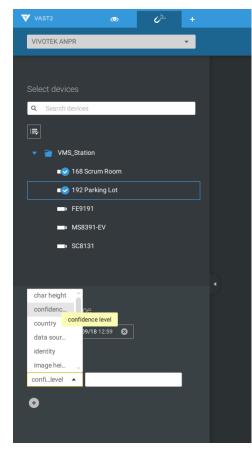
1. On the VAST live view, click on the Applications tab.

VAST2 +	сри 23% мем 80% 🏢 🐥 🌼 — Га 🗙
	🕶 Dashboard
	🛍 Е-Мар
	🞸 ^{h.} Data magnet
	VCA Report Data magnet
	Event search

2. On the Data Magnet window, select the LPR camera, and then begin with configuring the search conditions. Select the time span from the calendar. Select to display character height, country, data source, identity, image height, lane name, list name, or enter a plate number. You can select multiple filtering conditions.



VAST2)	C.	+	
VIVOTEK ANPR			•	
Select devices				
Q Search devices				
▼ 👕 VMS_Station				
■ C 168 Scrum Ro	om			
■ Serving Lo	ot			
■∎ FE9191				
■ MS8391-EV				
■ SC8131				
Select time frame				
09/02 12:59 ~ 09/18 12:59	8			
Search criteria				
		-		
confilevel 🔻 90 🛞		8		
€				



3. Click the Search button. The search results will display. Single-click to display the related video. You can also review the video in a full-screen mode.

▼ VAST2 @ 🗸 👘 +							CPU 47% MEM 87% 🎛 🌲 🍄 – 🗞
VIVOTEK ANPR	10,000+ results						∷ Ľ ∣ Ľ
						Carr	9/18/2019 12:40:27
Select devices	2019/09/18 12:40:17	4693 QB	4693QB	not in list	Taiwan	192	
Q Search devices	2019/09/18 12:37:11	0228 PT	0228PT	not in list	Taiwan	168 :	
▼ 🗃 VMS_Station	• 2019/09/18 12:36:31	0228 PT	0228PT	not in list	Taiwan	168:	· ·
■ v 168 Scrum Room	2019/09/18 12:33:44	0228 PT	0228PT	not in list	Taiwan		
■ FE9191	2019/09/18 12:31:56	0228 PT	0228PT	not in list	Taiwan		VIVOTEK ANPR
 MS8391-EV SC8131 	2019/09/18 12:31:02	0228 PT	0228PT	not in list	Taiwan		1C02.0D
	2019/09/18 12:25:01	0228 PT	0228PT	not in list	Taiwan		4033 ND
Select time frame	2019/09/18 12:21:37	0228 PT	0228PT	not in list	Taiwan		Plate number: 4693QB
	2019/09/18 12:15:47	0228 PT	0228PT	not in list	Taiwan		Timestamp: 2019/09/18 12:40:17
confilevel 👻 90 💿	2019/09/18 12:11:13	28-PT	28PT	not in list	Taiwan		List name: not in list
•	2019/09/18 12:10:57	28 PT	28PT	not in list	Taiwan		Camera: 192 Parking Lot
	2019/09/18 12:07:16	0223.07	0228PT	not in list	Taiwan		Data source: VIVOTEK ANPR
		< 1/	200				
9/18/2019	12:40:27	H	∢ ∥ н ∣				r

You can click and drag the display names of individual columns to switch their positions on the screen. The changes to layout are stored on the client computer. After you re-arrange the order of columns in search results, the display order will also be applied to the exported CSV file.

▼ VAST2 @ 6 ^{h.} +						CPU 10%	MEM 82%	∎ A ‡	- 15 ×
VIVOTEK ANPR	10,000+ results							<u>~</u> Ľ	
	29428	~							
Q Search devices									
▼ 🍵 VMS_Station									
■ Scrum Room									<u> </u>
■ Solution In the second seco	09/02 09	09/05 09/06 09/2	-418	09/09 09/10 Days					
FE9191	Timestamp	Plate image	Platenumber						
 MS8391-EV SC8131 		000000							
	2019/09/18 11:40:33	0228 PT	0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
	2019/09/18 11:38:25	0228 PT	0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
	2019/09/18 11:37:13	0228 PT	0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
III 09/02 12:59 ~ 09/18 12:59	2019/09/18 11:36:31	0228 PT	0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
Search criteria	2019/09/18 11:35:11	0228 PT	0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
confi_level 90	2019/09/18 11:33:23	5507- <u>1</u> 5	5507J5	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR		99.90
	2019/09/18 11:32:30	0228 PT	0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
	2019/09/18 11:31:38	0228 PT	0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
		0000			-				
<u>•</u>				< 1/200 >					

4. You can select and export a license plate capture using the Export function. Click on the export button. A folder button will display. Click on it to access the exported file.

♥ VAST2 @ (j ^{≞.} +						CPU 9%	MEM 80% 🏭 樽	. 🕸 – 🖻 ×
VIVOTEK ANPR	10,000+ results						≡ Ľ I	2 🖻
	Timestamp 2019/09/17 20:02:54	Plate image	Plate number 5823R8	List name not in list	Country Taiwan	Camera 192 Parking Lot	Data source Lan	e name Confide 90.03
Q Search devices	2019/09/09 10:07:53	2436622	263662	BLACKLIST	Taiwan	168 Scrum Room	VIVOTEK ANPR	90.03
	2019/09/18 10:11:36	28-PT	28PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR	90.04
 WMS_Station I68 Scrum Room 	2019/09/09 10:11:16	ARU-5168	ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR	90.05
■ FE9191	2019/09/17 12:45:27	ARF-5986	ARF5986	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR	90.06
MS8391-EV	2019/09/09 10:04:29	ARU 5168	ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR	90.07
SC8131	2019/09/09 10:03:24	ARU-5168	ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR	90.10
	4 2019/09/17 07:37:05	139512	1395L2	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR	
	2019/09/17 09:45:28	AAE 7339	AAE7339	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR	
B 09/02 12:59 ~ 09/18 12:59 Ø	2019/09/16 14:58:25	2436622	236622	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR	
Search criteria	2019/09/16 16:09:38	43 6622	436622	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR	90.14
confi_level v 90 C	2019/09/18 09:32:48	ATL 8600	ATL8600	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR	90.16
	2019/09/09 10:01:17	ARU-5168	ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR	90.21
	2019/09/09 09:53:21	ARU-5168	ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR	90.23
		C0:00//5			-			
				< 2/200	>			

The target directory will open. Open the exported CSV file to view the search results.

🗸 vast2 💿 🗸 👘 +								III 🐥 🌣	
VIVOTEK ANPR	10,000+ results Refine						≡ 2	I 🖆 👕	
	Timestamp P 2019/09/17 20:02:54	late image	Plate number 5823R8	List name not in list	Country Taiwan	Camera 192 Parking Lot	Data source VIVOTEK ANPR		Confide 90.03
Q Search devices	II ⊇ II = I File Home Share View	Manage Downloads Picture Tools				- 0 × n	VIVOTEK ANPR		90.03
루 🗃 VMS_Station	Pin to Quick: Copy Paste access	Move Copy Delete Rename New	™ New item * ■ Easy access * Properti	Edit Select	none	n	VIVOTEK ANPR		90.04
- 168 Scrum Room		ut to to folde Organize) > Users > Public > Documents > VIVOT			lect 오 전 Search		VIVOTEK ANPR		90.05
■ FE9191	OneDrive This PC	^ Name Mame 20190902_125916-20190918_12	916_VIVOTEK ANPR.csv	Date 9/18/2019 1:08 PM	Typ M Mic	pe Size crosoft Excel 逗點	VIVOTEK ANPR		90.06
■ MS8391-EV	 This PC 3D Objects Desktop 		Size	: Microsoft Excel 逗點分陽 13.7 MB : modified: 9/18/2019 1:08 F			VIVOTEK ANPR		90.07
■• SC8131	 Documents Downloads 						VIVOTEK ANPR		90.10
	Music Pictures Videos						VIVOTEK ANPR		
	🍆 OS (C:) 🗩 Data (D:)						VIVOTEK ANPR		
B 09/02 12:59 ~ 09/18 12:59 🔞	Network I item	v «			_	, n	VIVOTEK ANPR		
earch criteria	2019/09/16 16:09:38		436622	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		
	2019/09/18 09:32:48	ATL-8600	ATL8600	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR		90.16
	2019/09/09 10:01:17	ARU-5168	ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.21
	2019/09/09 09:53:21	ARU-5168	ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.23
		<u>E0500/3</u>			-				
🗠 🍯 🗊 🖩 🕺 🍳 ۹	N 10 10 10 10 10 10 10 10 10 10 10 10 10	2		1 0/000					1 9/

You can also open a chart view by clicking the Chart view button. The chart view can also be exported as a png file.

▼ vast2				CPU 13% MAAN 83% 🏭 🦺 🕸 – Fa 🗙
VIVOTEK ANPR	10,000+ results Refine otheria for better results			
Select devices Rearch devices Image: Constraint of the second s	29428 22071 14714 7357 0 0,002 09/03 09/04 09/05 09/06 09/07 09/08 09/09	99/10 99/11 99/12 99/13 99/14 Days	09/15 09/16 09/17 09/18	Doord data mager
■ FE9191		Plate number List name		VIVOTEK ANPR
MS8391-EV	Timestamp Plate image 2019/09/17 07:37:05	1395L2 not in list	Country Carr Taiwan 192	120512
■• SC8131	2019/09/17 09:45:28 AAE:7339	AAE7339 not in list	Taiwan 192	129212
	2019/09/16 14:58:25 243-6672	236622 not in list	Taiwan 168:	Plate number: 1395L2
Select time frame	2019/09/16 16:09:38	436622 not in list	Taiwan 168	Timestamp: 2019/09/17 07:37:05 List name:
	2019/09/18 09:32:48 ATL 8600	ATL8600 not in list	Taiwan 192	not in list Camera:
confi_level v	2019/09/09 10:01:17	ARU568 not in list	Taiwan 168:	192 Parking Lot Data source:
•	2019/09/09 09:53:21	ARU568 not in list	Taiwan 168:	VIVOTEK ANPR
	2019/09/18 08:56:13 7151KG	7151KG not in list	Taiwan 192∃	
	2019/09/09 10:01:54	ARU568 not in list	Taiwan 168	
<u>•</u>	< 2	/200 >		

Configuring Data Magnet alarms:

1. Enter Settings > Alarm > Add & Delete to create a new alarm setting. Click to select External devices.

VAST2	\$ +		CPU 29%	мем 78% 🏭 🌲	¢: - •a ×
🔊 Settings		Alarm m	nanagement		
				Q. Search alarms	
If	+ Add trigger	Do + Add action	At Add a schedule Always Customize	Alarm	Cancel
No.	Name	If the following By	Do	On/to At	*
1	168 Scrum Room	FE9191 ··· Motion dete Window 1	ction	Always	
_	_				_

2. Select VIVOTEK ANPR as your triggering source. Select and create triggering conditions such as character height, image width, list, list name, country, etc. Use "=" for text matching, "~" for text containing, or approximately matching specific characters, and also ">," "<," ">=," "<=" for text containing, or approximately matching specific characters, and also ">," "<," ">=," "<=" for numbers larger or smaller than a preset value.</p>

VAST2	¢ +	- C			8% MEM 78%	1 📖	. \$	
🔊 Settings			Alarm manaç	gement				
			Select trigger and	d source			×	
lf	Event/Status							
	Data magnet		▼ VIVOT	TEK ANPR 👻				
-	Set up trigger condition. Selec	t data and the type.	Then key in operator and keyv	words.			_	
	Data	Туре	Condition					Cancel
<u>*</u>	char height	Text	▼ Key in '=' for text m	hatch, "~" for text contain		0		
No.	€							•
1								
		hin 5 s						

3. Continue to configure your triggering conditions. You can create multiple conditions.

VAST2	\$	+							сри 2	22%	мем 73	7%		۹	\$		- 1	6 ×
🔊 Settings					Al	arm m	anag	ement										
						Select trig	gger and	source							×			
	Event/Stat	us																
If	Data magn	iet				*	VIVOTE	K ANPR	•									
-	Set up trigge	er condition. S	Select data	and the ty	/pe. Then k	ey in operato	r and keywo	ords.										
	Data		Ту	pe		Condition										Cance	ol	
<u>t</u>	char h	leight	•	Value	Υ.	>40 💿										Carice		
							&											
No.	count	ry	•	Text		=Taiwan	6						0	Θ				*
1	€																	
_			within	5 s														
			i i	1~30s														

4. Continue to configure the actions for a triggered alarm, such as sending live streaming.

VAST2	\$	+				opu 24%	MEM 77%	1 📖		\$		
🔊 Settings				Alarm m	anagement							
				Sele	ect actions				Į	×		
lf	Send live s	treaming		Ŧ								
	Select carr		нт	riggering camera							Add Cancel	

5. When done, enter a name for the alarm and click the **Add** button to complete.

VAST2	\$					% MEM 77			\$		
🔊 Settings	3		A	larm ma	nagement						
							Q Se	earch alarms	ş		
lf			Do		At						
-	Data Magnet			+ Add action	+ Add a schedu	le 168 S	crum Roor	m		_0	
	VIVOTEK ANP char height, cou		Send live strea	iming	✓ Always	Instru	uction			dd	
.*			Event triggering	g camera	Customize					Cancel	
No.	Name	lft	he following	Ву	Do	On/to		At			*
1	168 Scrur		OTEK ANPR r height, country	Data magnet	Send live streaming	Event trigg	ering ca	Alway	S		
2	168 Scrur		9191 idow 1	Motion detectio	n			Alway	S		
-											

6. You can now receive alarm notifications triggered by license plate recognition via the Data Magnet.

VAST2	\$	=• +	CPU 67% MEM 81% 🏥 🌲 🏚 🗕	
larm list/search	0 1	Æ	i 🖾 🗆 🗹	
			Group ala	arm
			Event type Time Star	itus
168 Scrum Room	VMS_Station	VIVOTEK ANPR - char heig	ht: 55.17(>40), country: Taiwan(=Taiwan) Data magnet 2019/08/22.15:13:14 New	(
168 Scrum Room	N VMS_Station	FE9191 - Window 1	Motion detection 2019/08/22 15:13:11 New	
168 Scrum Room	WMS_Station	VIVOTEK ANPR - char heig	ht: 75(>40), country: Taiwan(=Taiwan) Data magnet 2019/08/22.15:13:09 New	
168 Scrum Room	N VMS_Station	FE9191 - Window 1	Motion detection 2019/08/2215:13:06 New	
168 Scrum Room	N VMS_Station	VIVOTEK ANPR - char heig	ht: 55.17(>40), country: Taiwan(=Taiwan) Data magnet 2019/08/22.15:13:04 New	
168 Scrum Room	N VMS_Station	FE9191 - Window 1	Motion detection 2019/08/2215:12:58 New	
168 Scrum Room	N VMS_Station		Motion detection 2019/08/22.15:12:53 New	
168 Scrum Room	N VMS_Station	FE9191 - Window 1	Motion detection 2019/08/22 15:12:48 New	
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection 2019/08/22 15:12:43 New	
168 Scrum Room	N VMS_Station	FE9191 - Window 1	Motion detection 2019/08/2215:12:38 New	

Note that if you select "Include event-triggering camera" during the alarm configuration stage, the camera delivering the data source will be automatically selected.

VAST2	\$ +		CPU 20% MEM 77%	III 🐥 🌣	
🔊 Settings	Ala	rm management			
		Select actions		×	
If	Select camera Select camera Select camera C Search devices VMS_Station NV9411P FE9191 FE9191 FE919 FE9191 FE919 FE919 FE919 FE919 FE919 FE919 FE919 FE919	▼ ng camera	Add	Cancel	Add Cancel

Configuring Data Source macro via Send email and Send HTTP requests:

In **Settings** > **Alarm** > **Add & Delete**, Email and HTTP requests can be used to send data source macro to receivers. Use "
 " as the line break command. Note that an SMTP server should have been configured before the Email settings in Alarm.

+ Device na Trigger ty Event tim Storage p Station n Data Sou	vpe ne oath arre		You can sp notification	ecify multiple lir message.	nes of	inform	ation	in yo	ur al	larm
VAST2	\$ +				CPU 18% M	EM 81%	III A	۵	- 6	×
🔊 Settings			Alarm man	agement						
						٩	Search alarms			
lf			Select ac	ctions						
-	Data Magnet VIVOTEK AN char height, co	Send email	*							
			sieh7@gmail.com					Car	ICEI	
			Notification							
No.	Name	Even	erType: \$(TriggerType) tTime: \$(EventTime) igePath: \$(StoragePath) onName: \$(StationName) Source: \$(DataSource)				At Always		-	•
2	168 Sc			-			Always			
3	Alarm		apshot image Test				Always			
_					Add	Cancel	-			

Appendix F: Enable Smart Tracking for Speed Dome Cameras

The Smart tracking function is available on speed dome cameras, such as SD9374-EHLX. The Smart tracking feature is separately configured on the camera side. Please refer to Smart Tracking User Guide for configuration details.

To display Smart tracking on VAST,

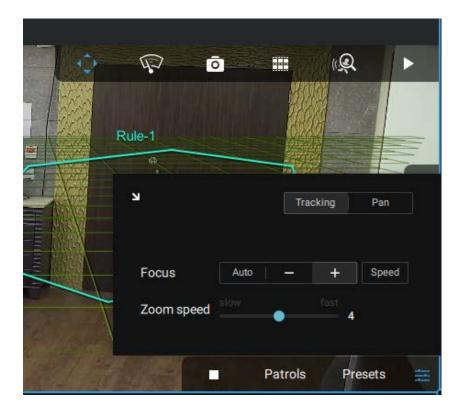
- 1. Enter Settings > Devices > Cameras.
- 2. Select the speed dome camera that supports this feature.
- 3. Select PTZ Settings, and the Track mode menu. Select **Smart tracking** as the tracking display mode. A hyperlink is provided for the Smart tracking configuration page.

It is recommended to always enable "Enable track if the camera idles for xx seconds." Manual PTZ control always has a higher priority and will interrupt tracking.

4. Click the **Apply** button.

VAST2	o 🕸 +			сги 15% мем 19% 🏭 🌲 🏟 —	∿ n
🔊 Settings			Device management		
Cameras Sites Sites Di/Di/Di/devices Di/Di/Di/devices Di/Di/Di/devices External devices	 escrittaria 	Basic Video Image Motion detection PTZ Settings Multicast €€	PIZ default ON PIZ operation mode Click to move Continuous move Track mode Before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filment filmeking The before starting please configure filmet fil		

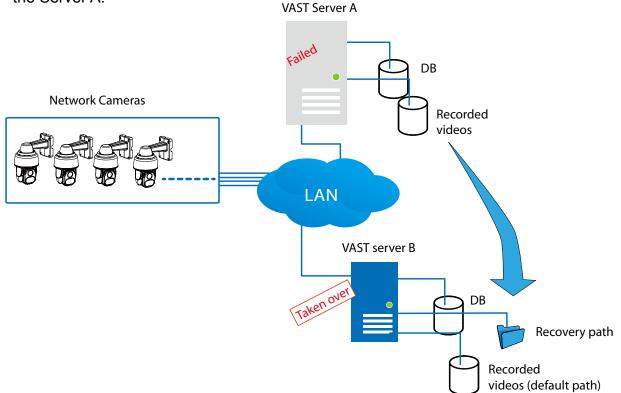
5. On the view cell of the speed dome, click PTZ settings, and then click the Tracking button.



Appendix G Database Merge Function

The Database Merge function applies in the following scenario:

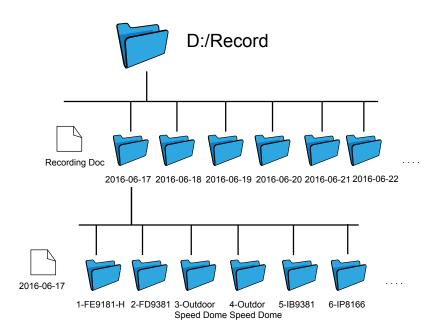
1. A VAST server A failed or was intentionally depleted. The precondition is that the disk drives containing the recordings remain intact. Server B must also have the configuration profile of the Server A.



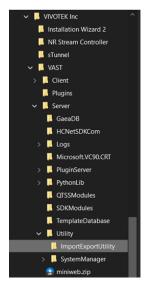
2. The VAST server B is used to continue video recording. The previous recordings on server A can be retrieved by attaching the hard disk(s) to server B or manually copying to a storage device on server B. You can then designate the location of these files as the "Recovery path" from server B. An administrator can then use the VAST software to access the past recordings.

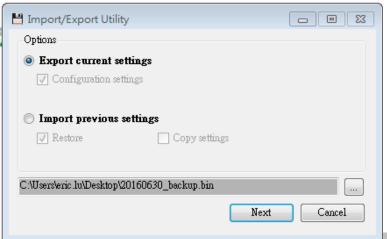


- It is **IMPORTANT** to move or copy the entire storage group folder, e.g., D:/recording/2016-06-17/1-FE9181-H..., which is a root directory configured by VAST server as the recording folder. The default recording folder contains file folder structure, video files, and database metadata. If you copy the video files only, the database data will not be synchronized, and you will not be able to access the recordings.
- The video streams received from cameras will not be recorded on to the Recovery path folder. It is designed to maintain previous recordings. The Recovery path folder becomes static.



 It is also a good habit to export and preserve your VAST system configuration to prevent losses in the event of system failure. In case you want to migrate or upgrade your VAST server, you can use the Import-Export utility to duplicate your VAST configuration to another server. Copy the configuration file and import the configuration from another VAST server.





When the file folder is ready for server B, designate the location of recovered files from another VAST server, go to Settings > Recording management > Recording options.

Select the recording folder that contains the recordings from the counterpart VAST server. Select the **Restore recordings from this path** checkbox and click **Add**.

VAST2	o 🕸 +			. Ⅲ ♣ ✿ - ℡ ×
🔊 Settings		Recording m	anagement	
Recording options	 UMS_Station 	Archive name DefaultGr Server	NAS X	i
Backup Failover Local DB	DefaultGroup	Select a folder	C:/ 42.29 GB available of 136.6 GB	Recycle Options
			Restore recordings from this path Add Cancel	Seamless recc
				Auply Cancel

The Local Database you incorporated will be listed on the device tree, which is separated from your current deployment. There are two different scenarios"

1. Using Recovery path:

Server B incorporated Server A configuration file, selected Recording options and the "Restore recordings from this path" option. The device tree will look similar to the original VAST server A configuration.

2. Using Local DB:

A Local DB sub-folder will appear on the device tree. Click to select the cameras in the sub-folder to access the past recordings. The recordings in the Local DB is only accessible from the computer which has a copy of the Local DB.

For system backup options, refer to page 284.