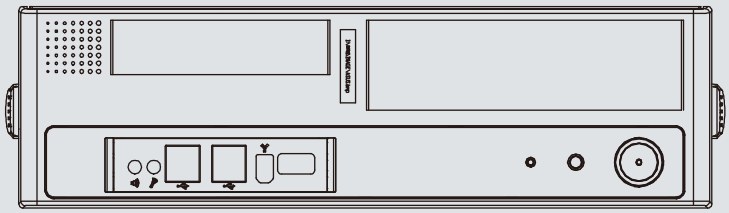
NS9521 VAST2 Station

User's Manual

Industrial Compact Enclosure • 32 CH expandable to 64 CH • VAST2 Inside
DVI/HDMI/DP • 2x HDD Bays • Full Integration with VIVOTEK Cameras



Rev. 1.0
for VAST rev. 2.6

Table of Contents

Revision History

Rev. 1.0: Initial release. The description for the software functionality is based on VAST rev. 2.6.

⚠ WARNING:

1. Do not format or initialize the disk 0: drive on your system. 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.

⚠ WARNING:

Power cord shall be connected to a socket-outlet with earthing connection.

⚠ WARNING:

This equipment is intended to be used in a Restricted Access Location. A restricted access area can be accessed only through the use of a special tool, lock, and key, or other means of security.

The access can only be granted to service persons or by users who have instructed about the reasons for the restrictions applied to the location and about any precautions that shall be taken.

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.

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。」

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.

NOTE:

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

Package Contents

- NS9521
- Power cords
- Foot pads
- Mouse
- Quick Installation Guide
- Screws and slide rails

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 machine.

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

NS9521 is a VAST2 station that comes with pre-installed VAST2 recording software. The station supports all VIVOTEK camera models, including the latest 5-Megapixel and fisheye cameras.

The unit is equipped with two gigabit Ethernet RJ45 ports which provide network failover functionality to avoid the risk of recording loss. Up to 2 HDDs can be installed in the system.

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 system on handheld devices. Integrated with all of VIVOTEK's network cameras, VAST2, and iViewer software, users can realize a fully-featured and robust surveillance system. This ingenious station 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
- 2 x HDD bays
- 2 x Gigabit RJ45 Ethernet ports
- 8 (USB 3.1 Gen 2 Type-A, USB 3.1 Gen 2 Type-C, 4x USB 3.1 Gen 1, 2x USB 2.0/1.1)
- Size: 330 (H) x 96 (W) x 365 (D) mm
- 32 CH Live View and Playback, expandable to 64 CH
- H.265/H.264/ MJPEG
- HDMI x1, Display port x1, DVI x1.
- PTZ Support
- Snapshot / Export Media
- PiP Video Control
- Bookmark Design
- Fast Configuration Backup / Restore
- Pre-installed VIVOTEK VAST2 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 qualified personnel 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.

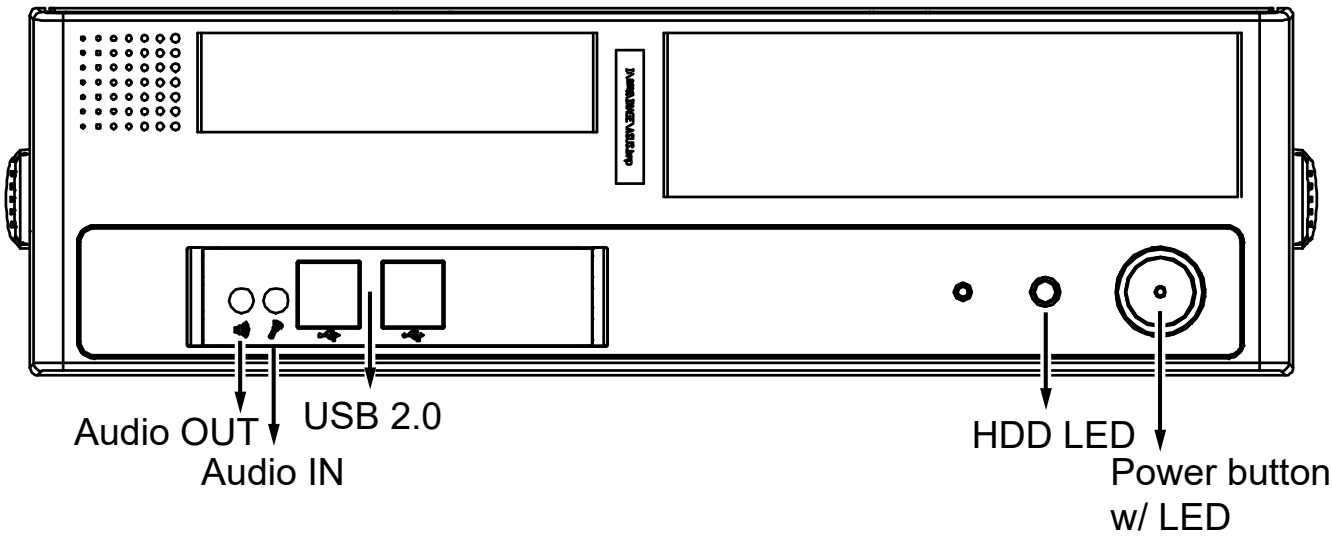
Warning:
When installing the product, use the provided or designated connection cables, power cables and AC adaptors. Using any other cables and adaptors could cause a malfunction or a fire.Electrical Appliance and Material Safety Law prohibits the use of UL or CSA -certified cables (that have UL/CSA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

Power Supply

Watt	300W max. (80+ Bronze, PFC)
Input rating	100 ~ 240 Vac ~ 5A, 50-60Hz
Output voltage	+5V sb @ 2.0A, +12 V @ 18A, +5V @ 16A
Safety	UL/TUV/CE/FCC class B

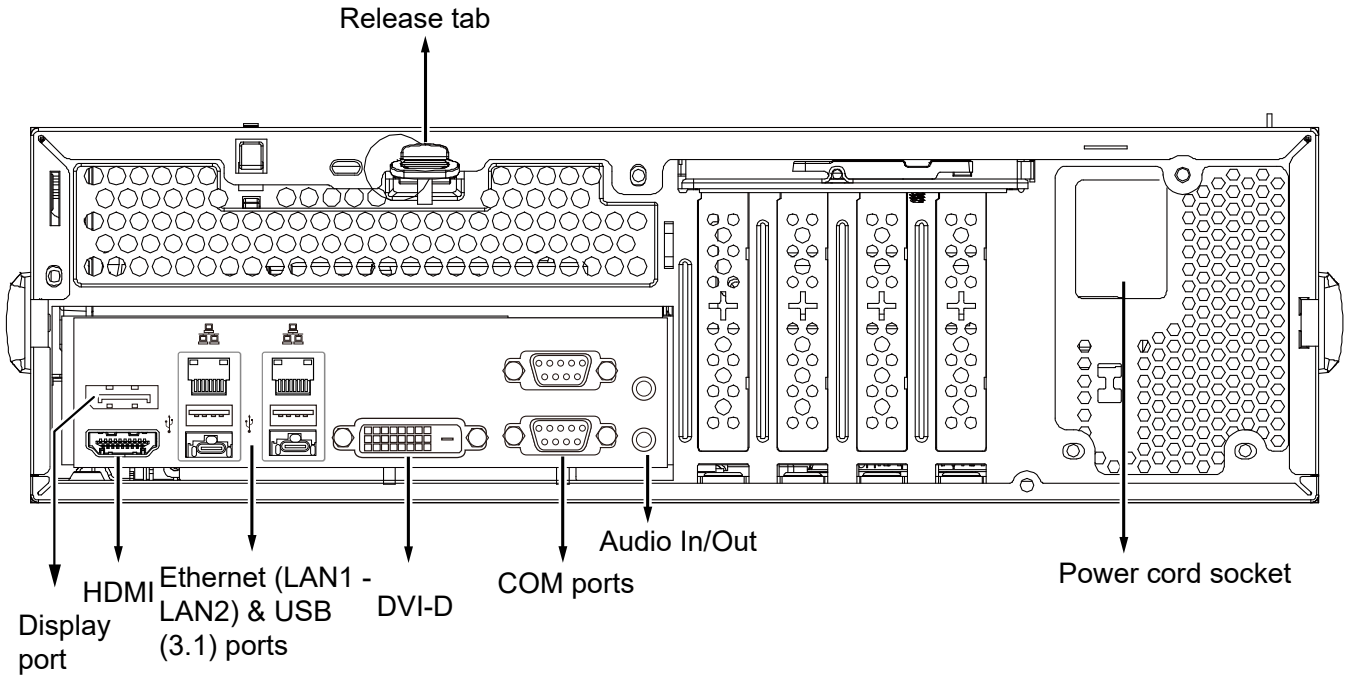
Physical Description

Front View



Control Panel buttons and LEDs			
	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.	
	HDD LED*	Blinking: data access.	N/A
		OFF: idle	N/A

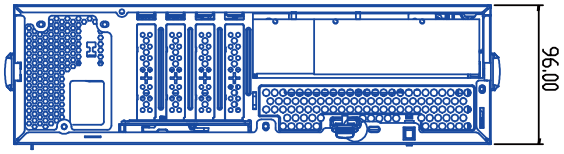
Rear View

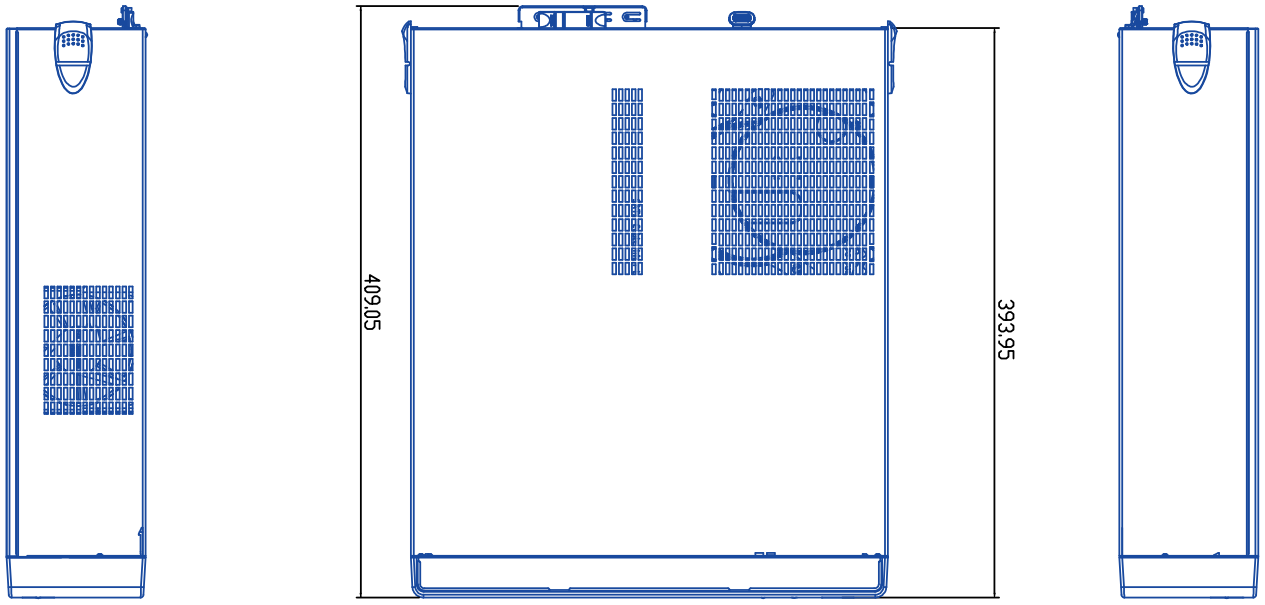

Release tab
Display port
HDMI
Ethernet (LAN1 - LAN2) & USB (3.1) ports
DVI-D
COM ports
Audio In/Out
Power cord socket

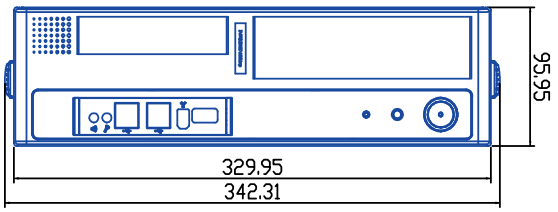
Display

Interface	Resolution
HDMI	Supports max resolution HDMI 2.0 4096 x 2160 @ 60 Hz
DVI-D	Supports max. resolution 1920 x 1200 @ 60 Hz
Display port	Supports max resolution 4096 x 2304 @ 60 Hz

Chassis Dimensions





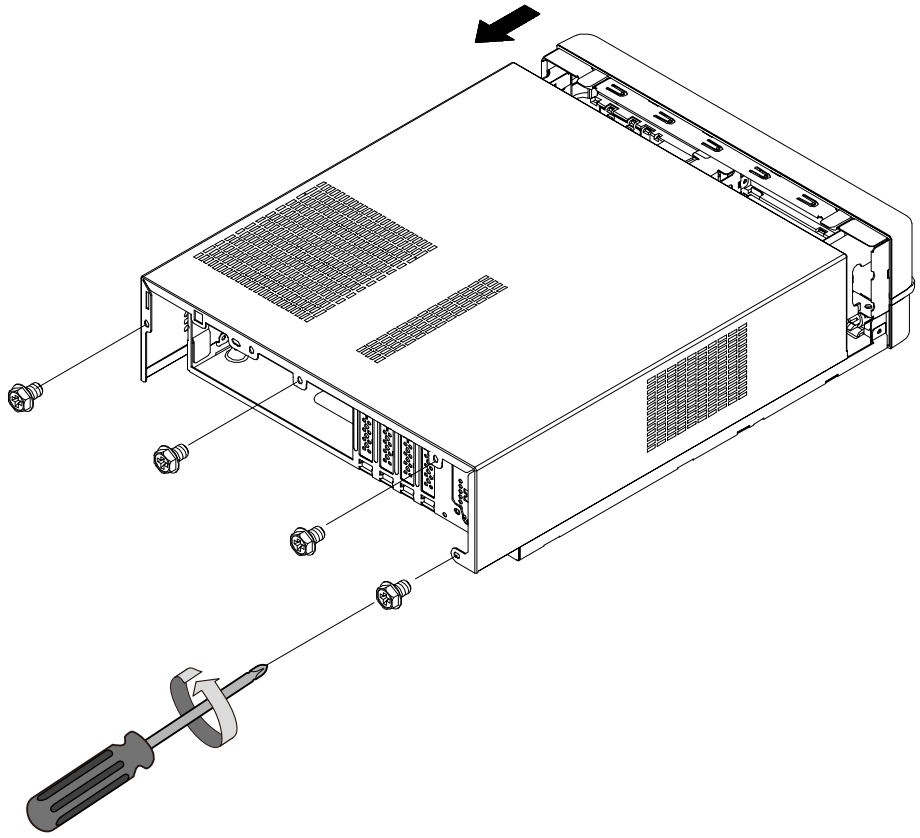


Installing Hard Disk Drives

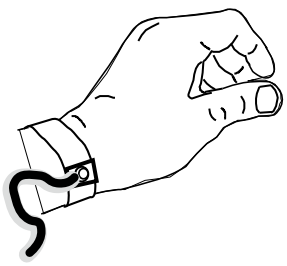
IMPORTANT:

- Avoid touching the hard drive's circuit board or connector pins. Doing so can damage the hard drive by electro-static discharge.

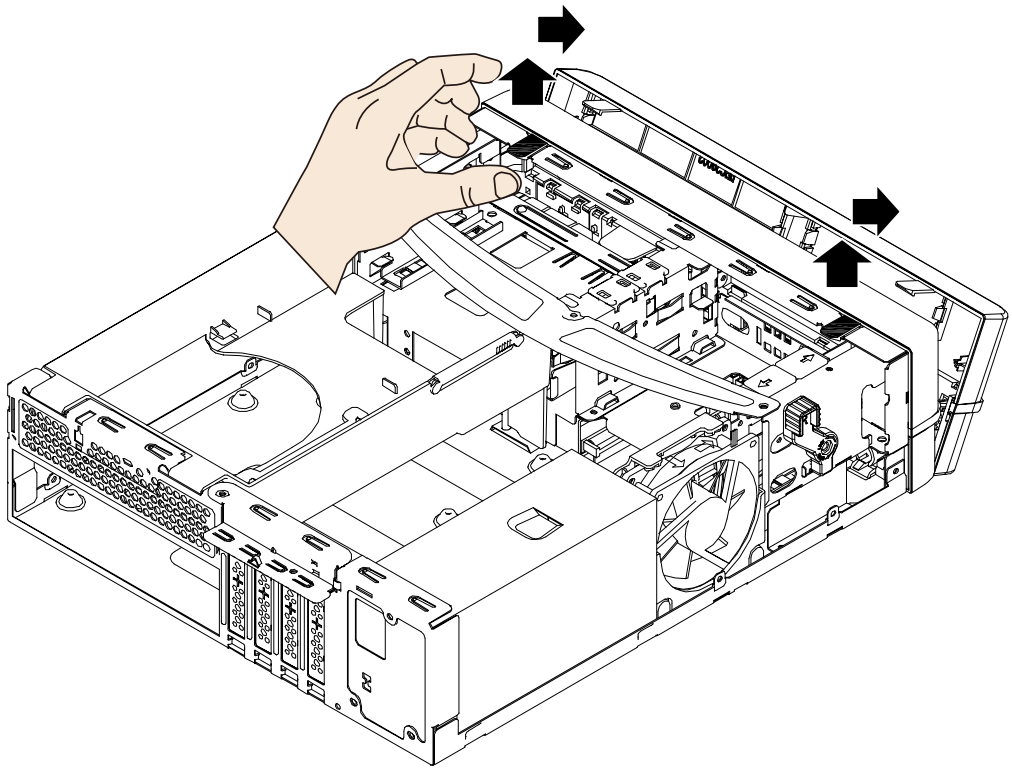
1. Remove top cover by loosening the screws from the rear of the chassis. Slide the top cover backward.



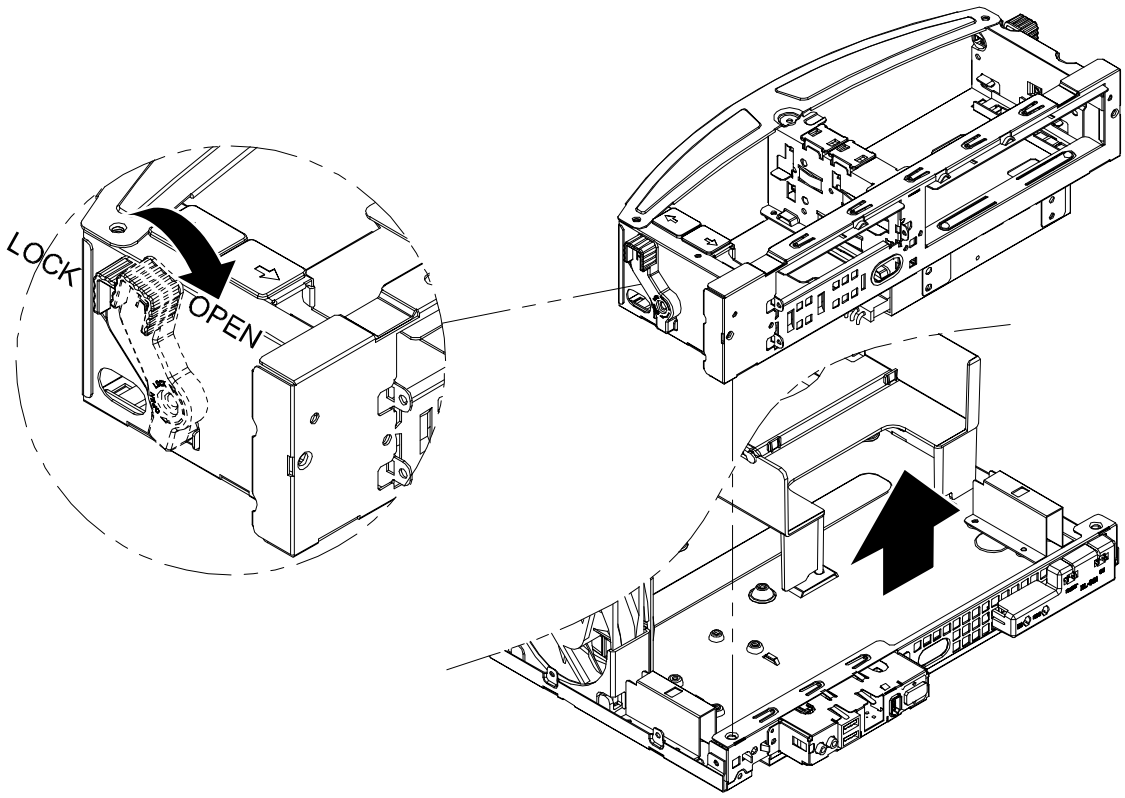
It is recommended to wear an anti-static wrist strap when handling hard drives.



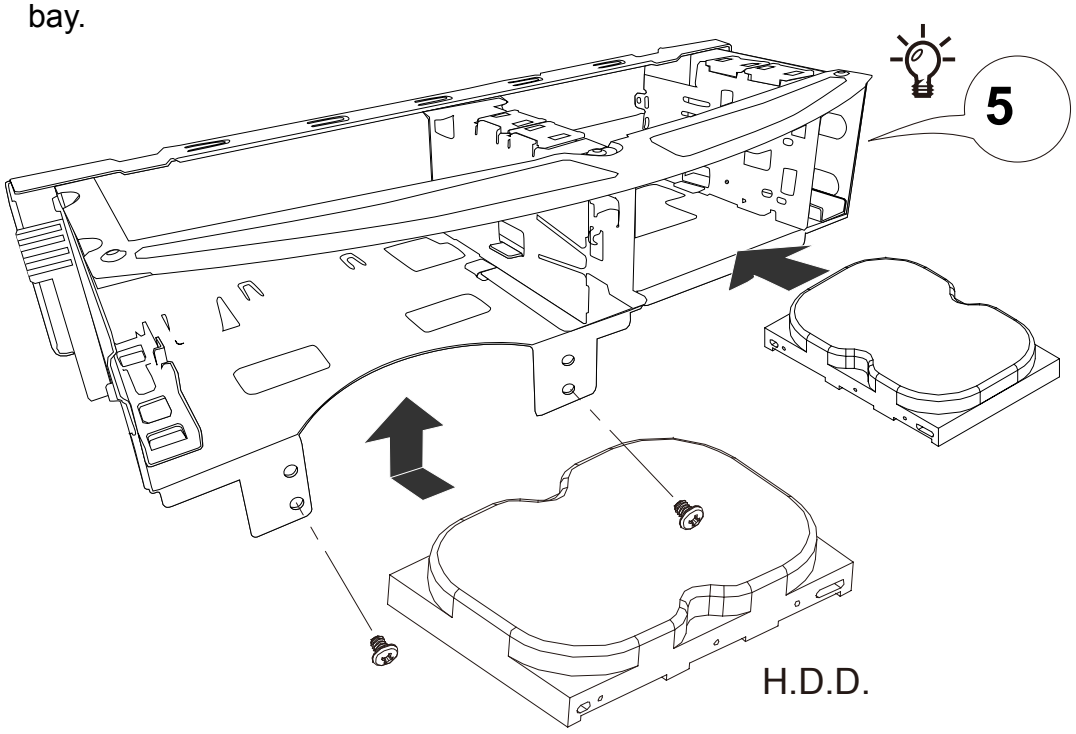
2. Remove the front bezel by lifting its tabs and push forward.



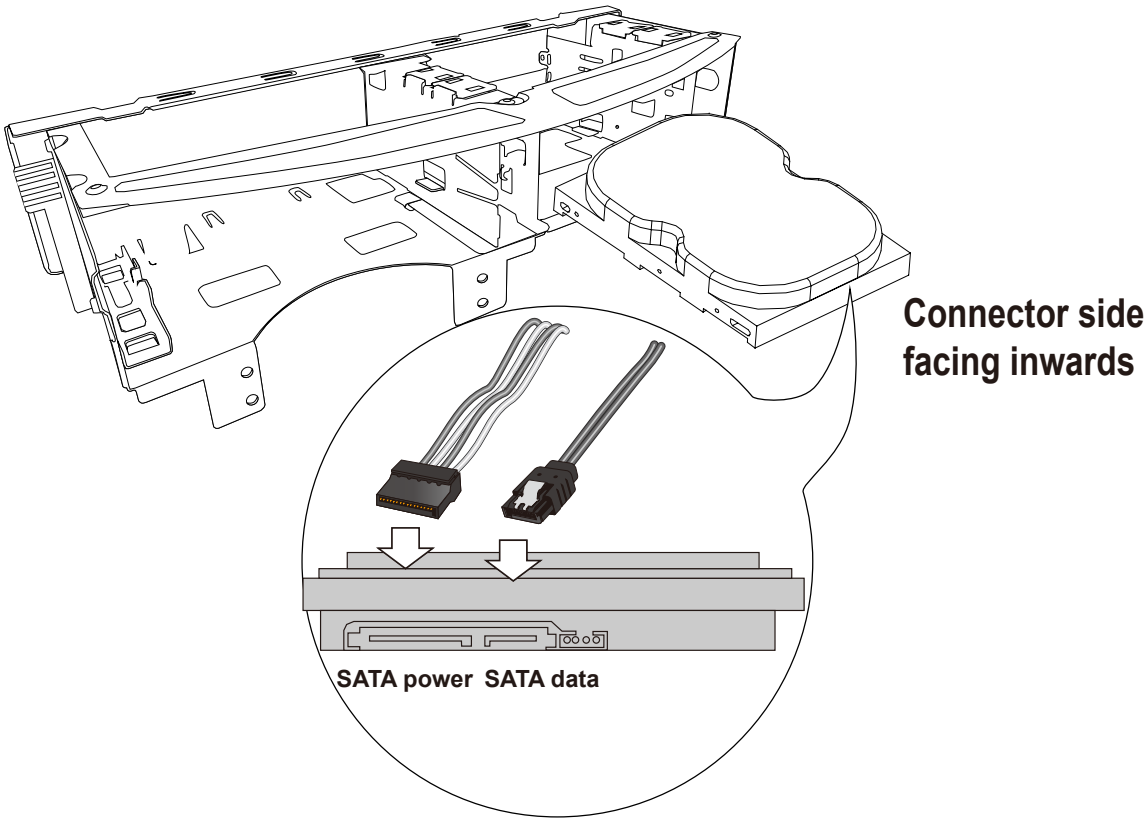
3. Pull the retention levers on the sides and remove the front section bracket.



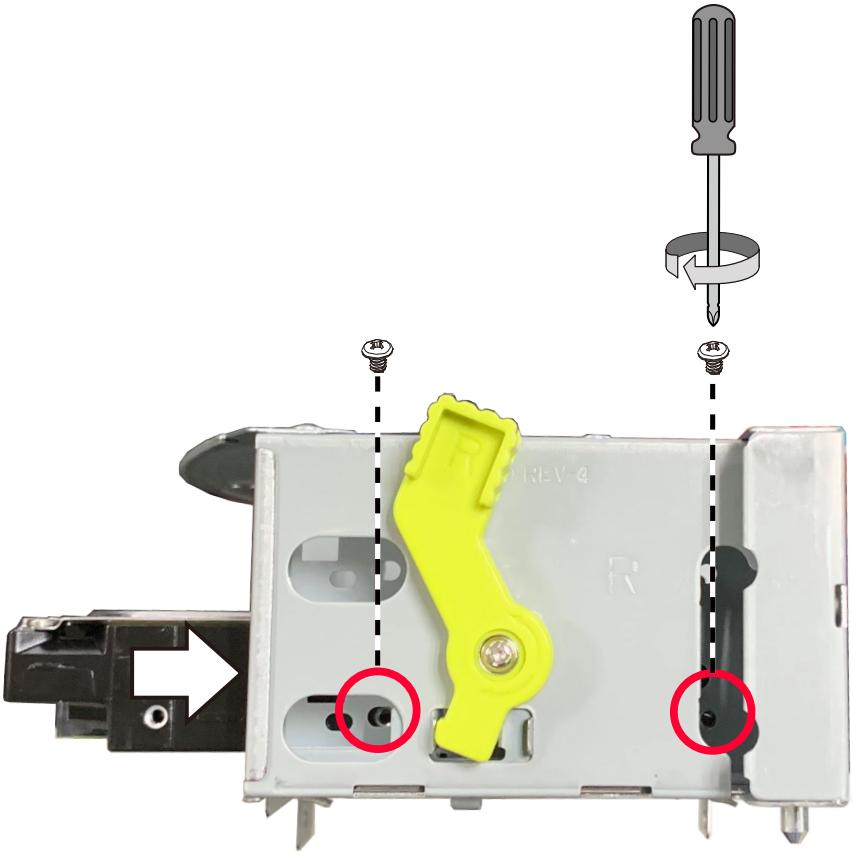
4. Install 2 hard drives to the locations indicated below: 1. under the bracket; 2. into the drive bay.



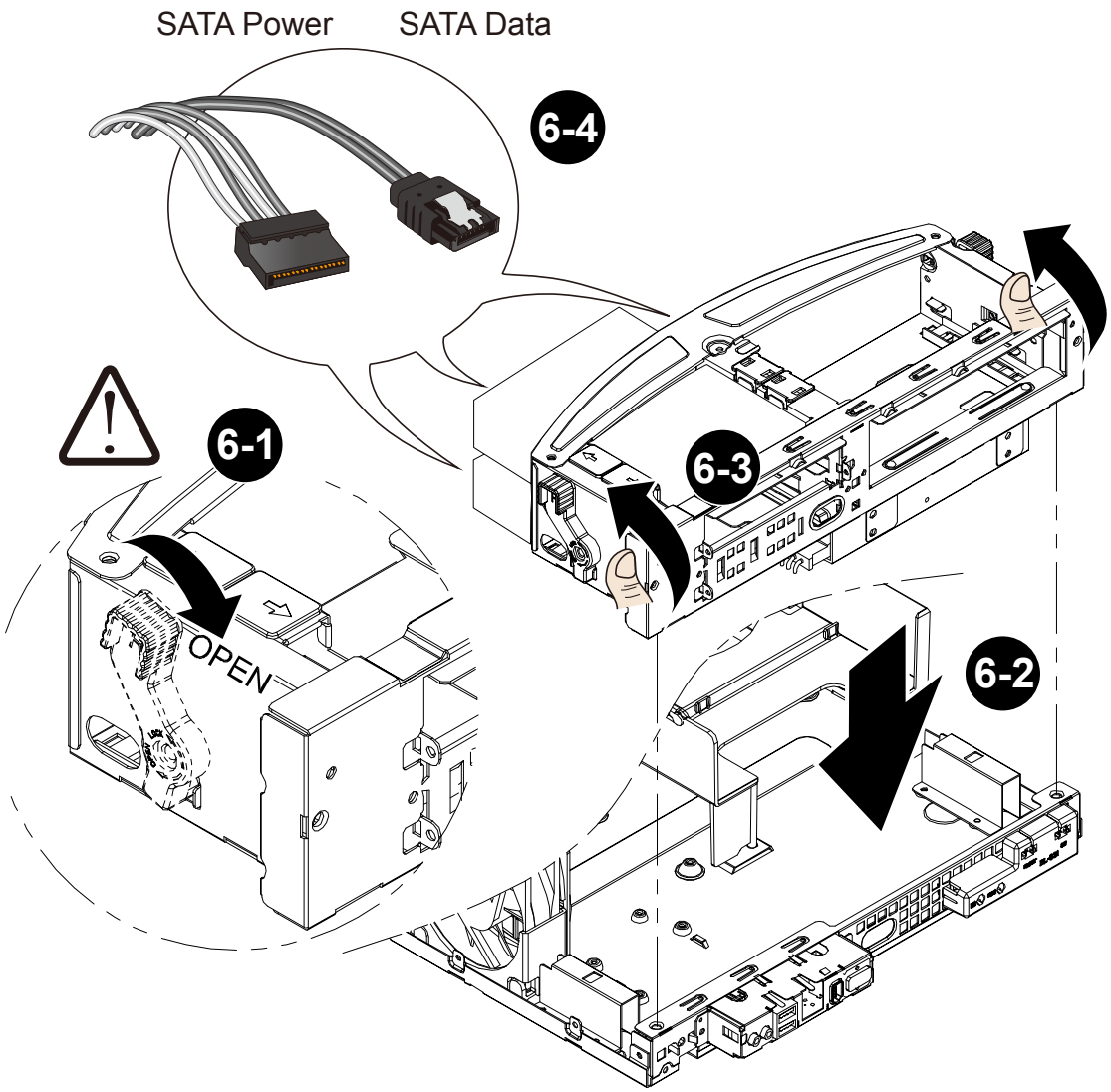
Note that the connector side of the hard drive should be facing the inside of the chassis.



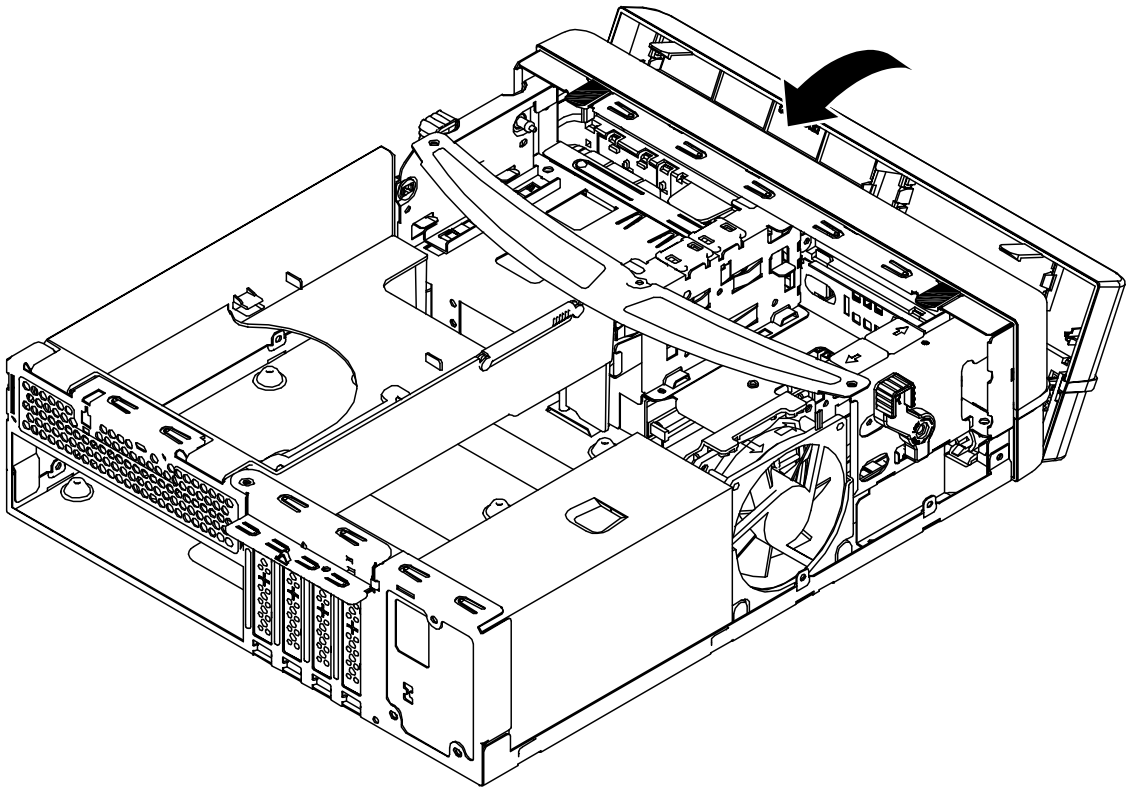
5. Secure the hard drive in the drive bay from the side of the bracket. See the through holes below.



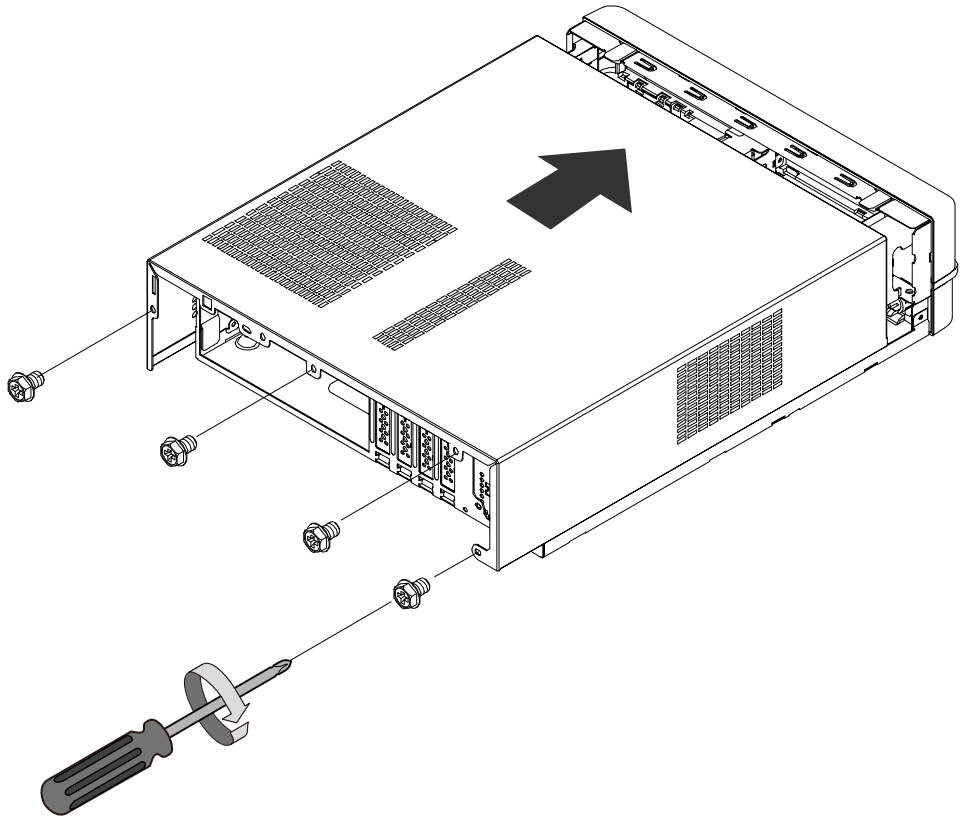
6. Install the bracket assembly.
6-1. Aim the guide pins underneath the bracket with the holes on the chassis. Make sure the levers are at the OPEN position.
6-2. Lower the bracket into its original position.
6-3. Once seated, push the levers to the locked position.
6-4. Connect the SATA Power and SATA Data cables from the main board to hard drives.



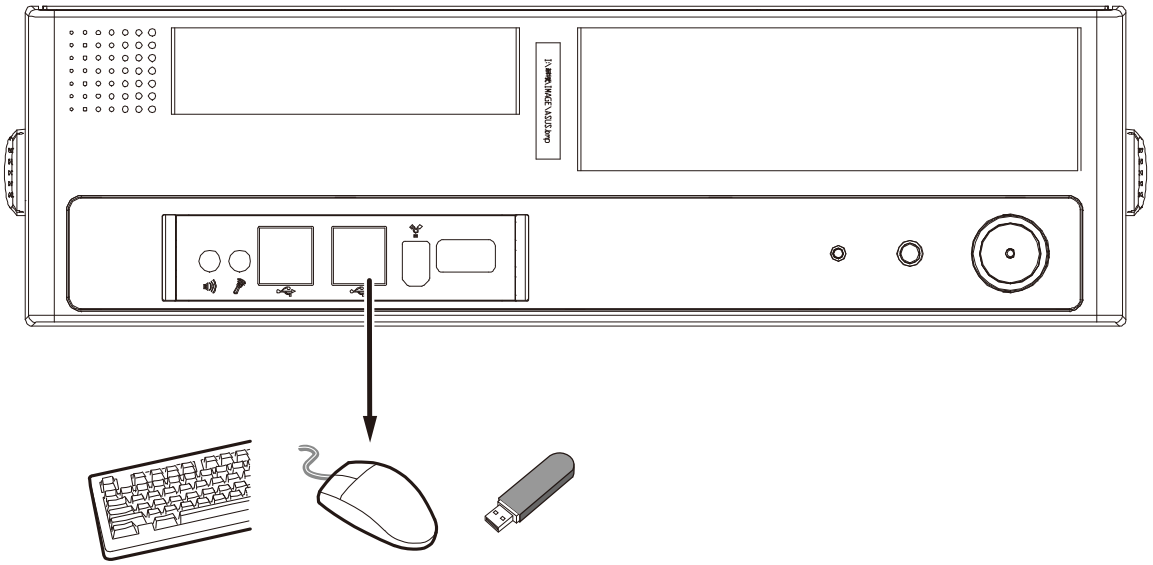
7. Install the front bezel by aligning the bottom first and push to fit to the front section bracket.



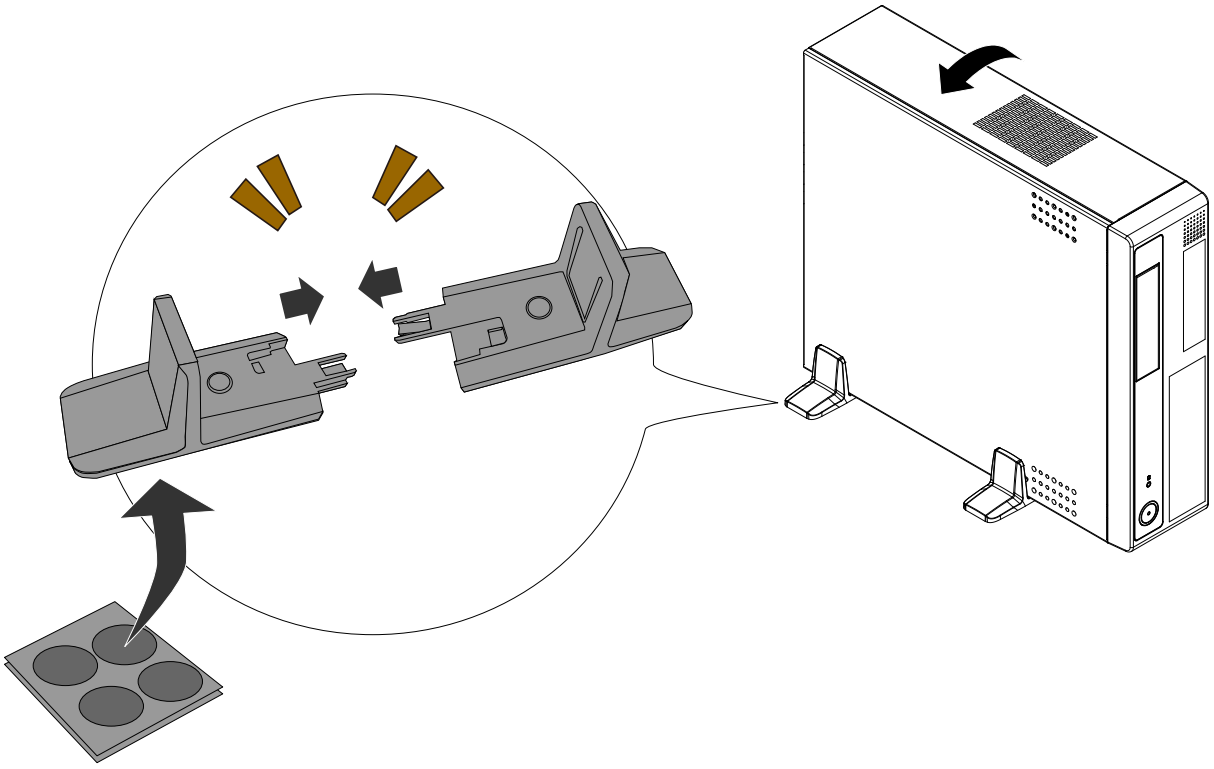
8. Install the top cover by sliding it into place and fasten the retention screws.



9. Connect a keyboard and mouse to the USB ports.



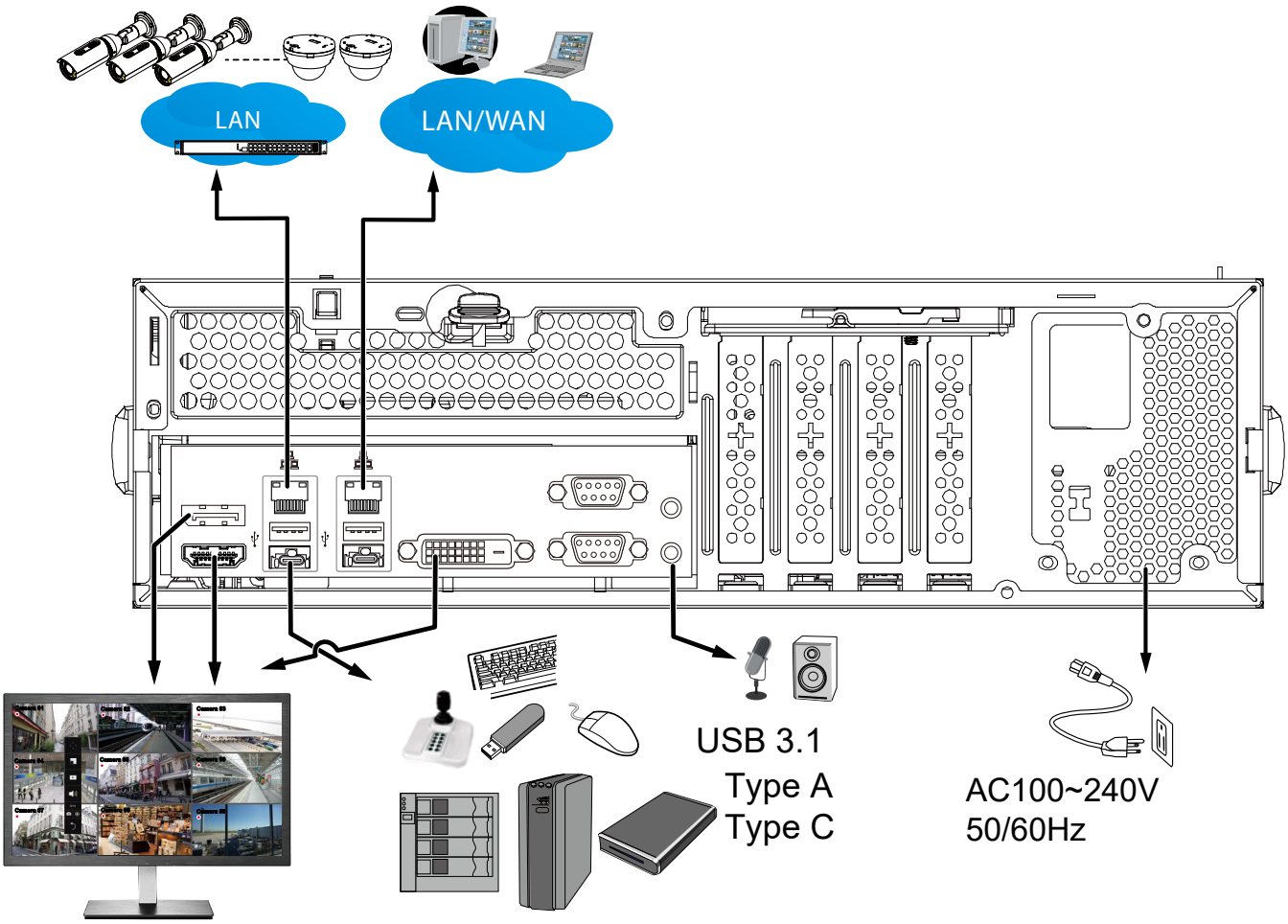
10. Assemble the plastic foot pads by snaping them together. Attach the rubber stickers to the bottom of the foot pads. You can then place the chassis in a standing orientation.



Connecting Interfaces

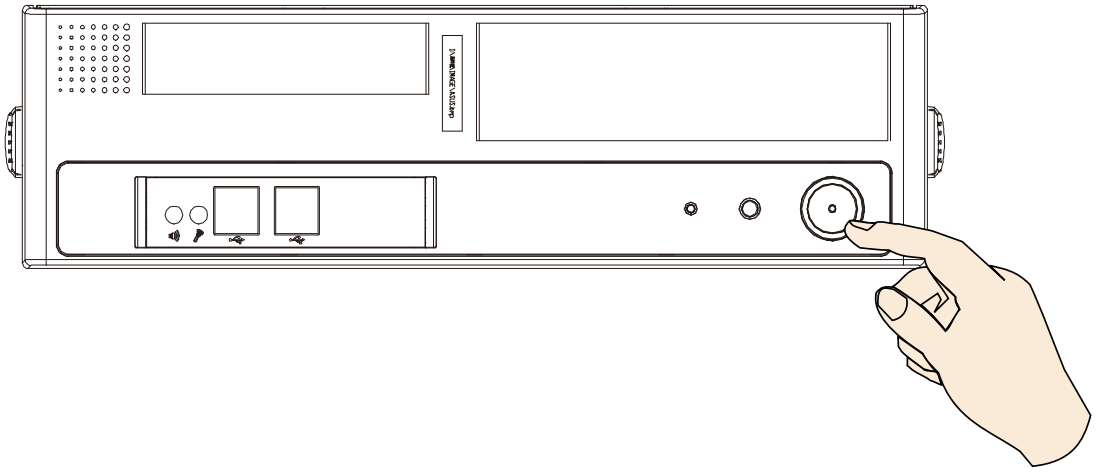
Refer to page 12 for the interface connections.

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 the power supply to power mains.

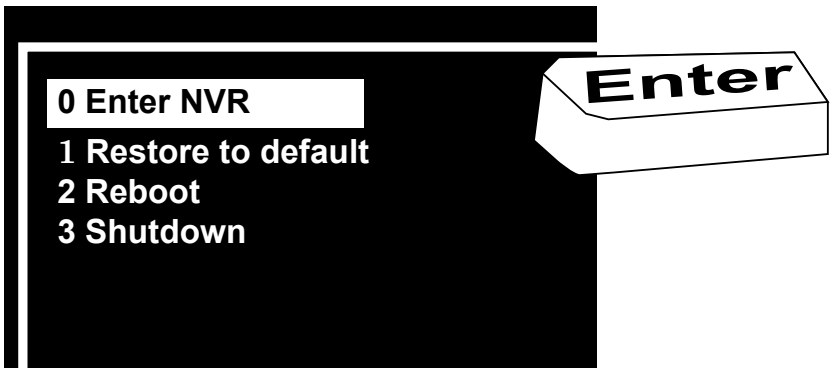


Initial Configuration

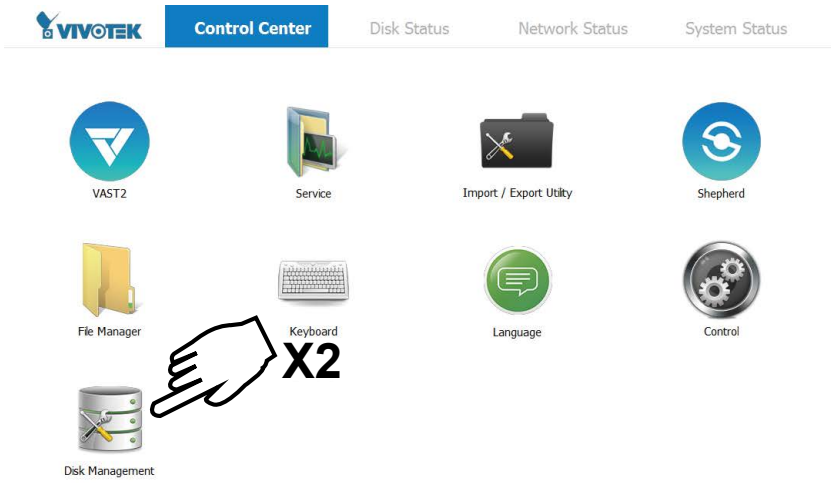
1. Power up the system by pressing the power on button.



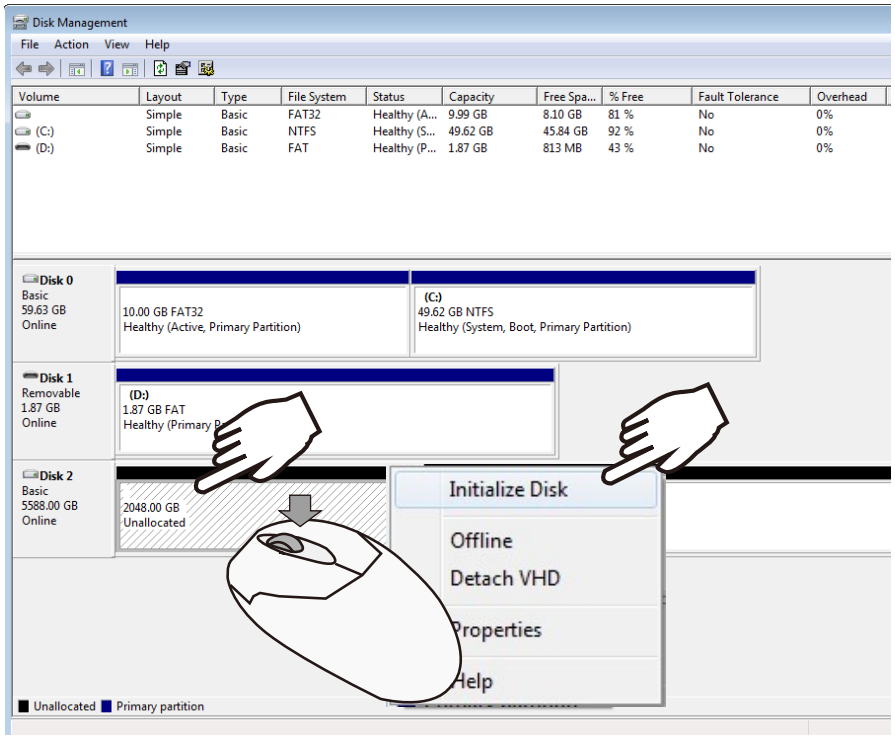
2. Skip the BIOS screens and select **Enter NVR** at the selection screen. The system will start. Wait for the start-up process to complete.



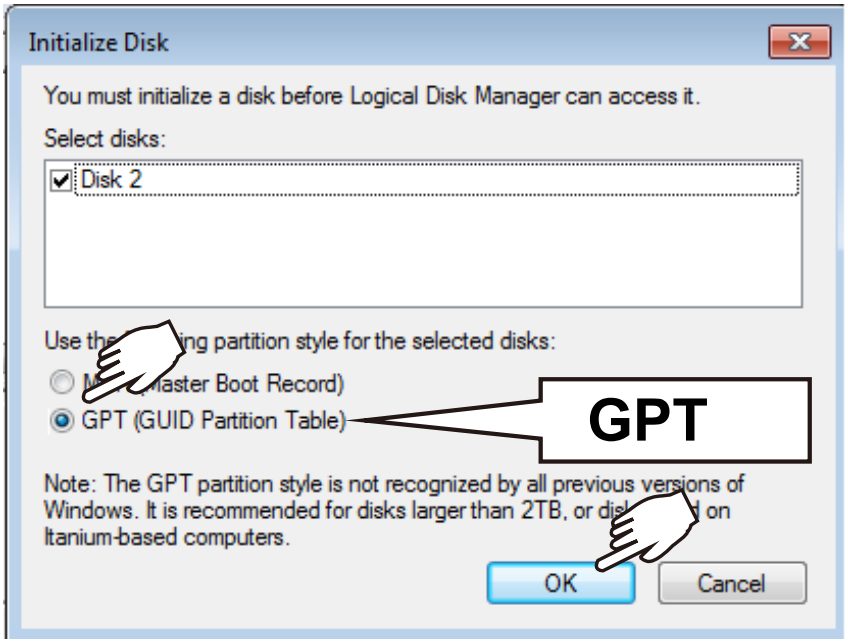
3. The system will boot up to the system main screen. Double-click on the **Disk Management** shortcut to start the Disk management utility.



4. The hard drives you installed should appear a new disk partition Disk 1 and Disk 2. 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.

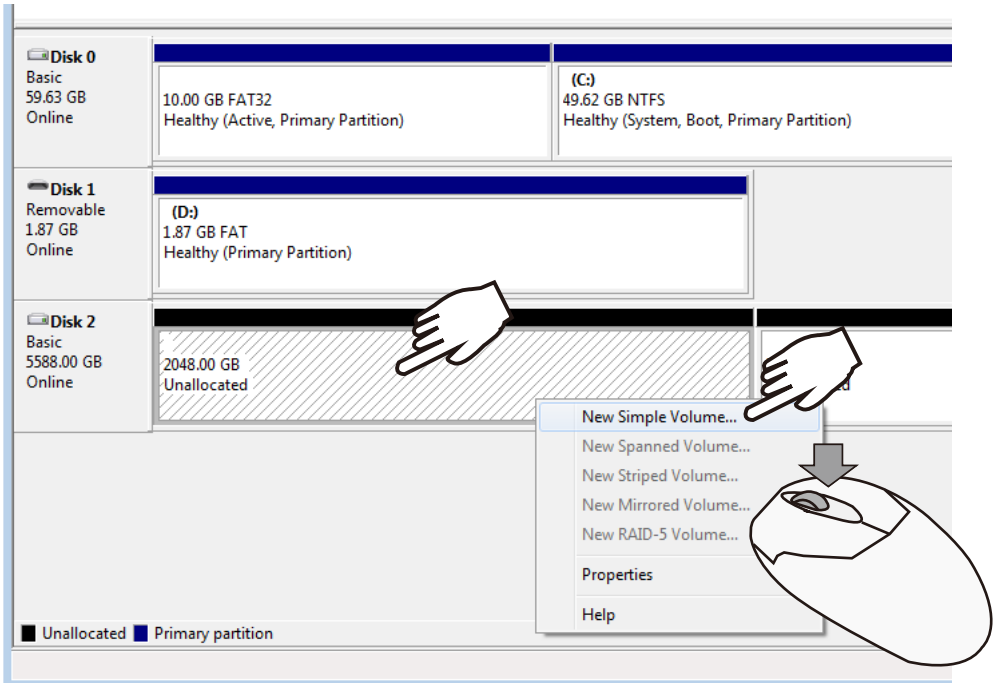


5. Select **GPT** (GUID Partition Table), and then click **OK** to proceed. This window may automatically pop up when Disk Management is started.

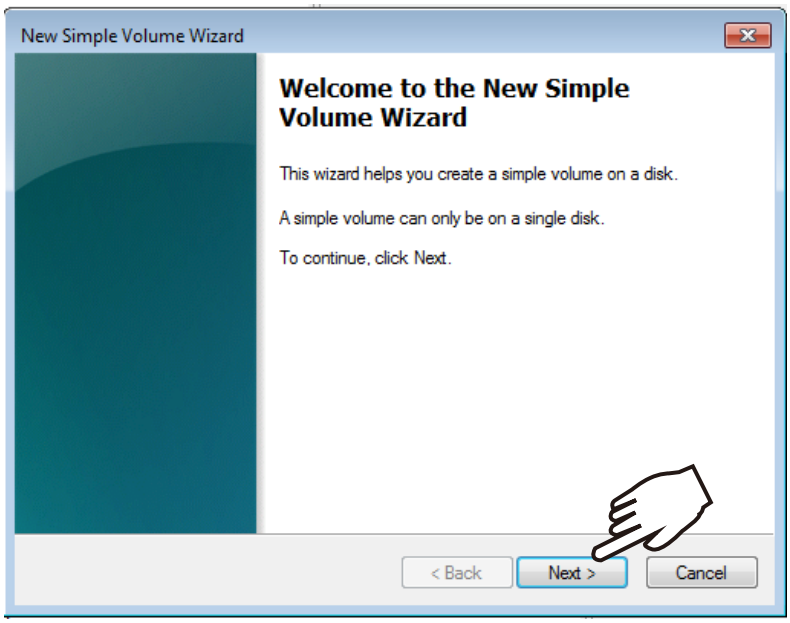


6. Once initialized, you can create a new volume**.** Right-click to display the **New Simple Volume** command. Click to proceed.

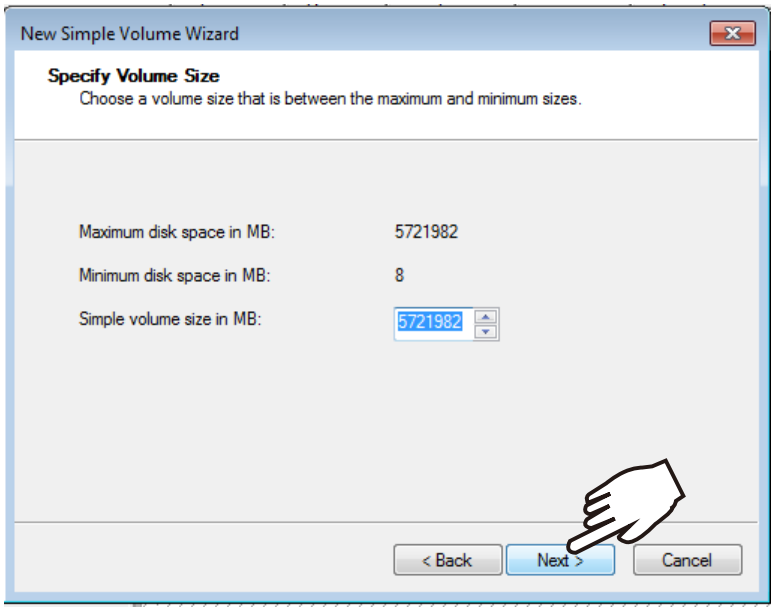
   Please do not format drive C:. Doing so will disable the system.



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

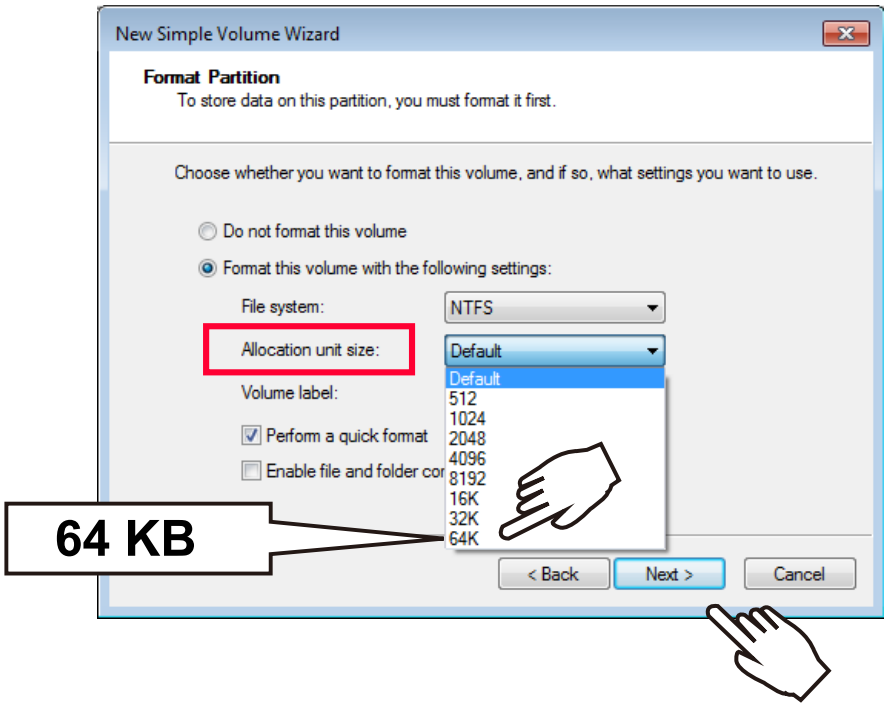


8. Leave the volume size unchanged. Click Next to proceed.

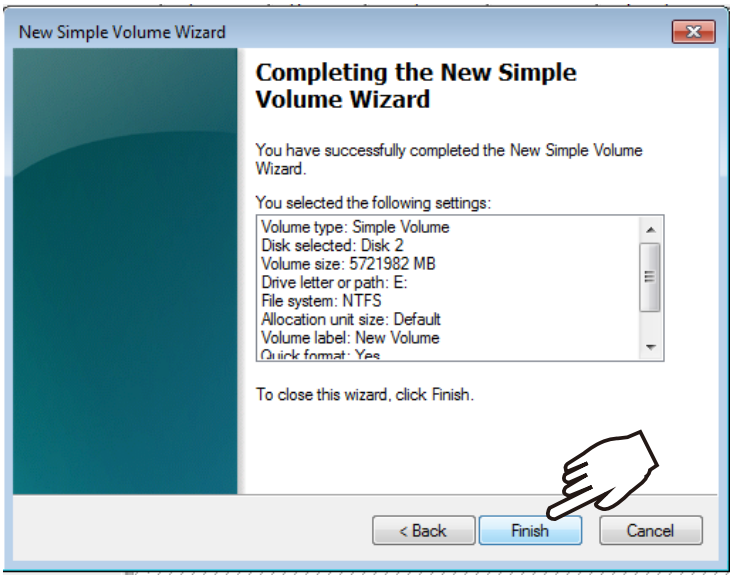


9. When prompted to assign a drive letter, click Next to proceed.

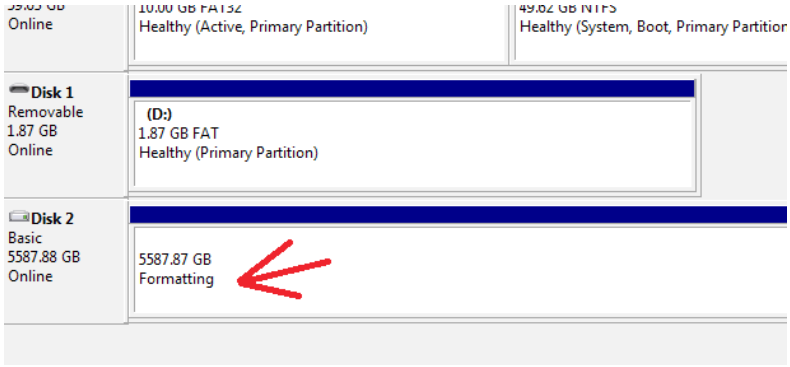
10. On the **Format Partition** page, select the **Allocation unit size** as **64KB**. When done, click Next to proceed.

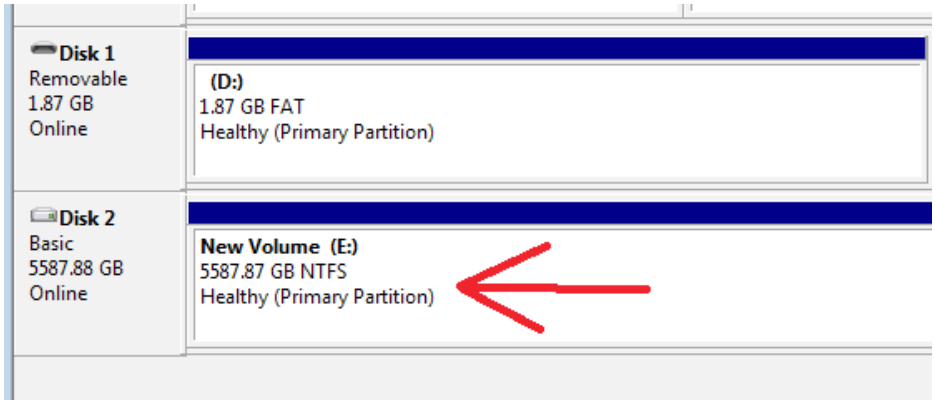


11. Click Finish to end the wizard.

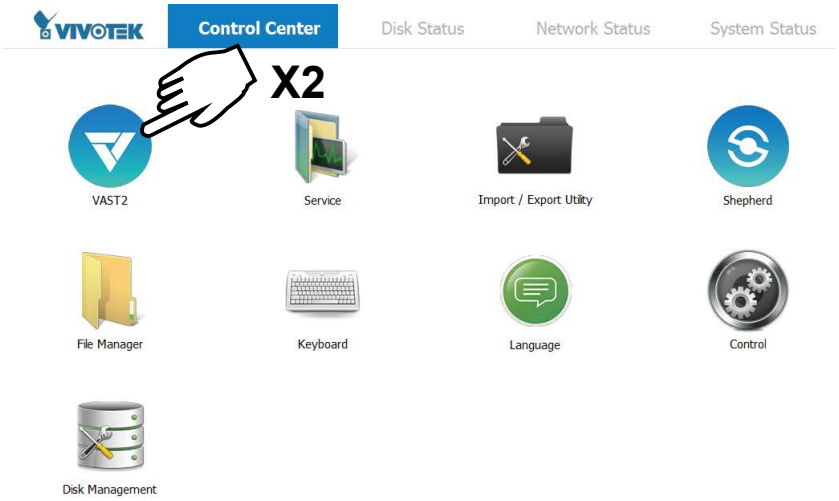


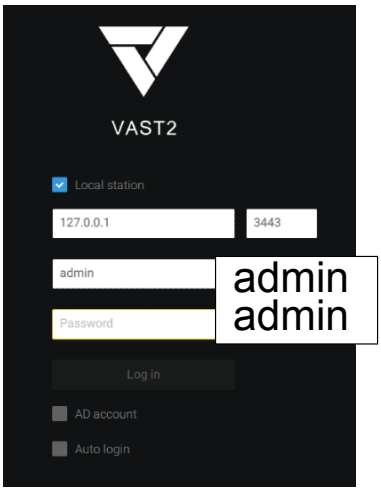
12. The formatting process will run in the background. When done, the new volume shall be indicated as a healthy new volume. Close the Disk Management window.





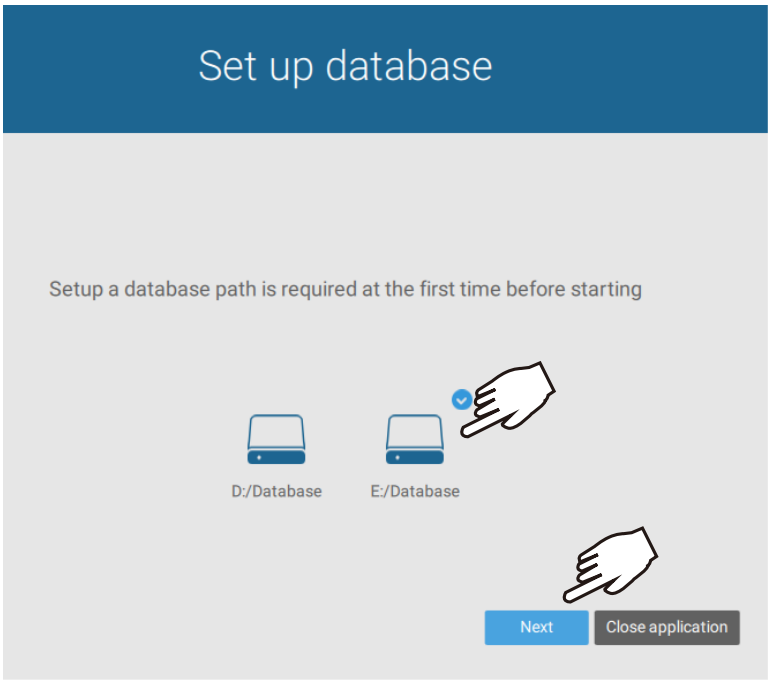
13. Start VIVOTEK **VAST** management software by double-clicking its shortbut. Enter **admin** and **admin** as the User Name and default Password. You can change the password later in the utility. Click **Log in** to proceed.



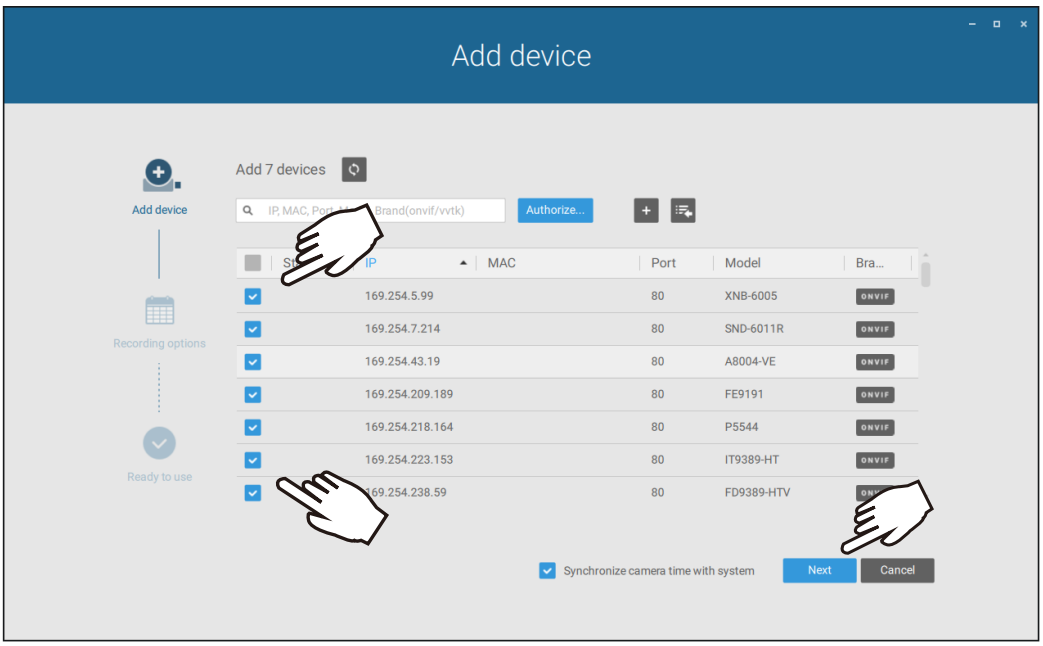


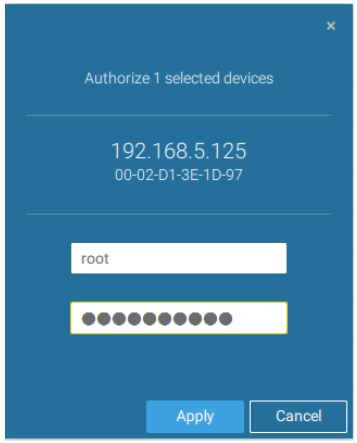
Top row	Control Center: the default desktop. Disk Status: Displays the current storage volume status (system drive and disk volumes). Network Status: Displays the information for the current network connections. System Status: Displays the current system status, license information, and VAST service.	
Desktop Shortcuts		
	VAST2	Starts the VAST2 recording and management software.
	Service	Enables you to start, stop, or restart the VAST server instance.
	Import/Export	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 Managment	Starts the Disk Management utility in Windows.
	RAID Config.	Not functional for this model.

14. 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.

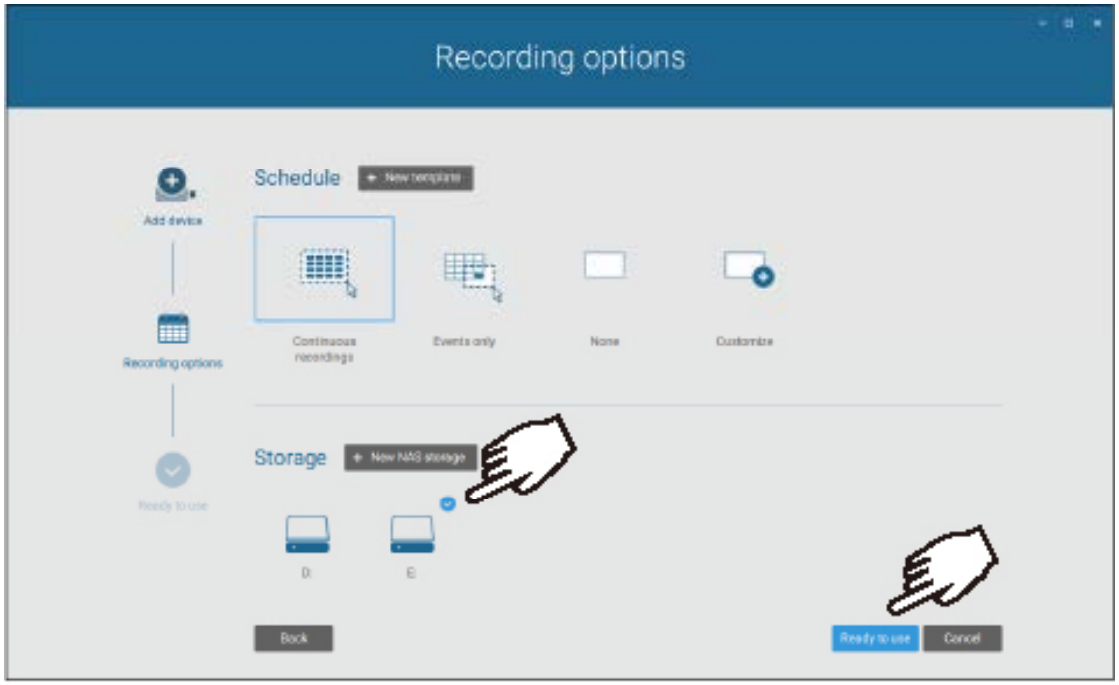


15. The next screen provides a list of all cameras in the local network. Select the cameras of your choice. Enter the credentials for making the connection with the network cameras. When done, click the **Next** button to proceed.

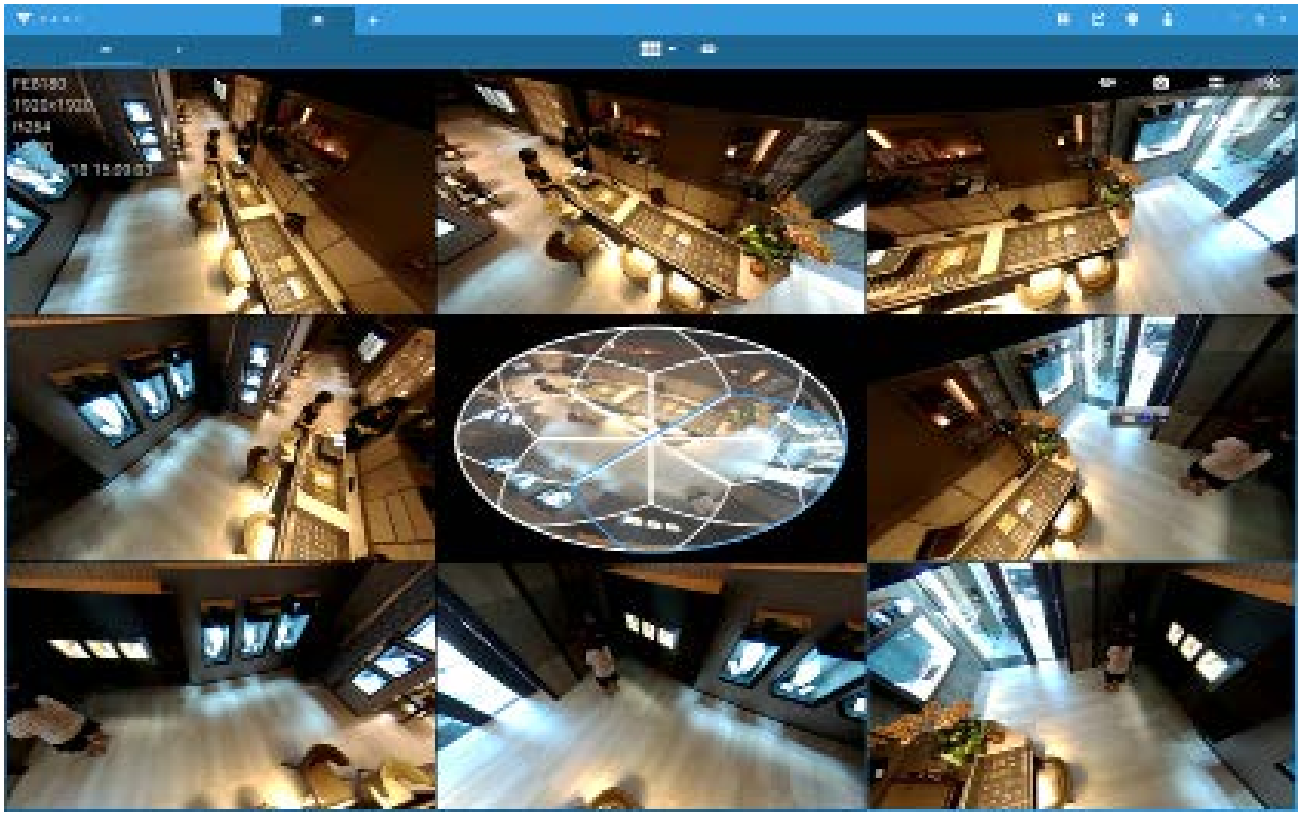




16. Select the recording volumes, such as the E:/ volume you just created. When done, click the **Ready to use** button.



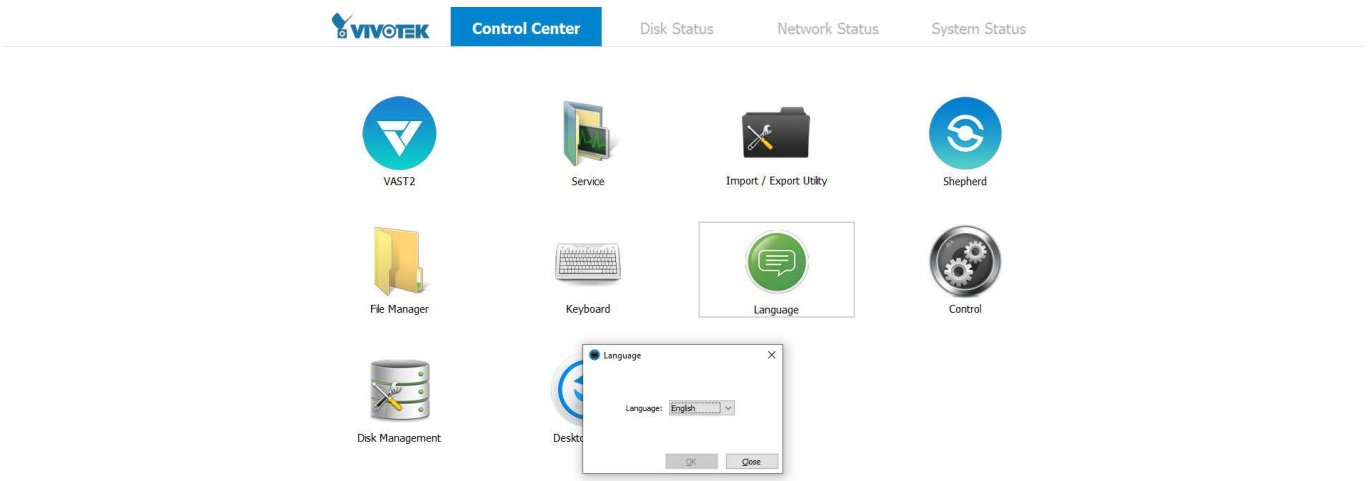
17. You should then enter the Liveview of the VAST2 software. Follow the discussions in later sections for how to configure your VAST2 deployment.



NOTE:

1. Cameras and the station must reside in the same subnet. Otherwise, the station 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.

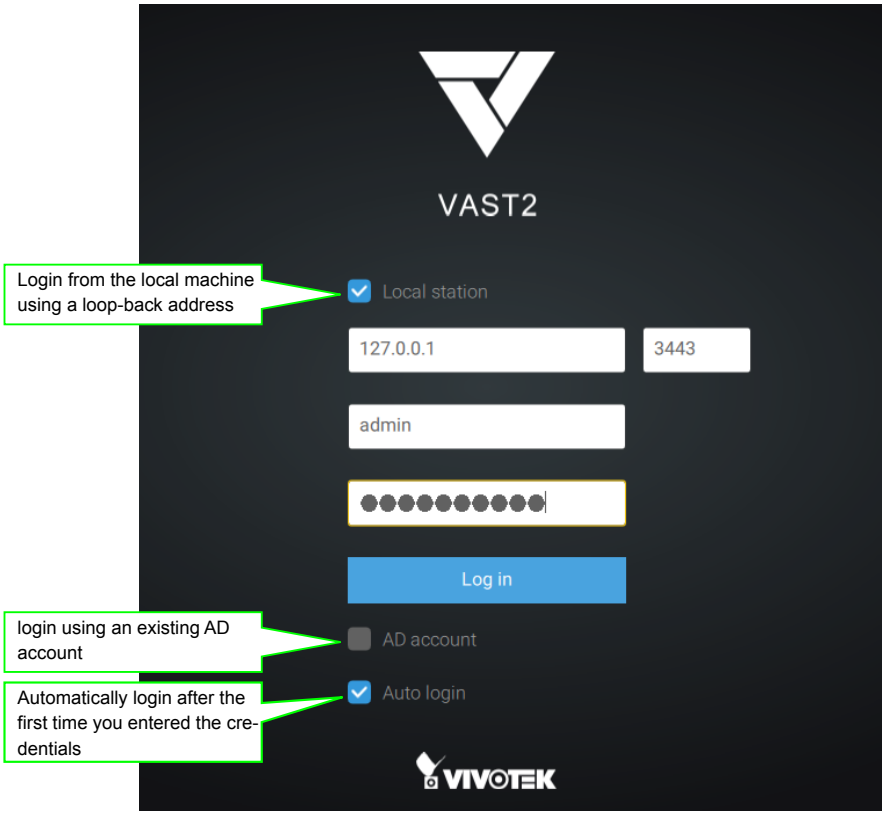


Chapter Two VAST2 Software Configuration and Management

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 199 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

- License Plate Recognition Solution & Data Magnet
  - Shows Data: Displays license plate related data in Live View
  - Edits Display Data: Select which types of data should be shown.
  - Search: Links data with recordings
  - Chart View: Display the search results in line graph.
  - Export: Exports the search results as CSV and PNG files.
  - Alarm: Triggers a alarm when data in certain columns are matched with the preset criteria.
  - Includes Event-Triggering Camera: Sends the live streaming from event-triggering cameras to the Alarm Tab when a alarm is triggered.
  - Data Source macro" Use Data Source macro in actions, such as “Send email” and “Send HTTP requests”.
- Alarm Grouping: One Click to Organize Enormous Number of Alarms
- Mute Alarm Notifications
- Easy-to-Use Interface for MAC License Users
- Multi-Sensor Display Modes: 1P, 1R, 1P2R, 1P3R

Key Features

- Cybersecurity Management Solution
- Smart Search II: Powerful people search in one click.
- Smart VCA: AI Powered Video Analytics
- Multi-Monitor Support with Tabbed Windows
- Evidence Lock: Automatically Bookmark Related Recordings When Alarm Triggered.
- Evidence Export: Manually Export Video Recordings or Alarm Clips.
- New Matrix for Video Wall Solution
- Automatic Problem Feedback Mechanism
- Multiple Fisheye Dewarp Modes
- System Overview Dashboard
- Add-on Solutions: Failover, Transportation, Transaction and Data Magnet

* 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:

- 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 needs to be imported on the 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.

Advanced Feature License:

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

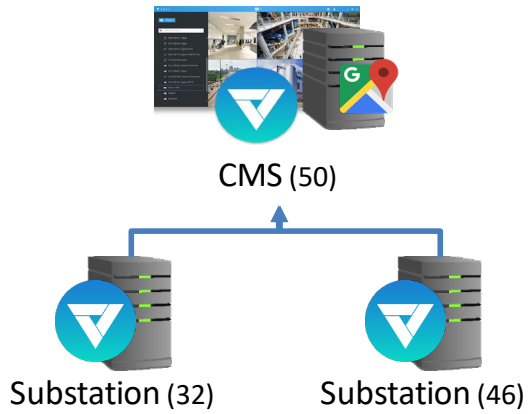
  NOTE:
  1. Failover license cannot be used on hardware dongle.
  2. The related configuration pages/menus will still be available even the license has not been activated.

Calculation - Transportation Package: Google map + GPS

Single Server (50)

Total no. of cameras: 50
Needs 50 packages.

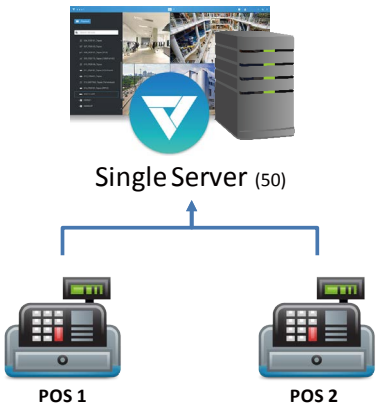
NOTE: camera normal usage licenses are included.



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

NOTE: camera normal usage licenses are included.

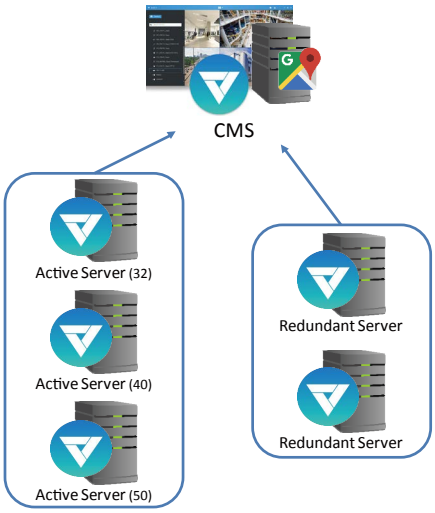
Calculation - POS License



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



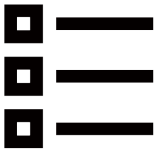
Rule:
No. of channels on the active server hosting the largest no. of cameras x the no. of redundant servers.

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)



Alarm list (50)

- 10 TCP messages
- 20 camera motion
- 20 DI trigger

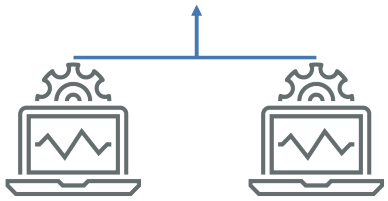
Rule:
The no. of licenses depends on how many alarm rules are using TCP Message as the triggering source.

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

Single Server (50)



3rd party SW

3rd party SW

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).

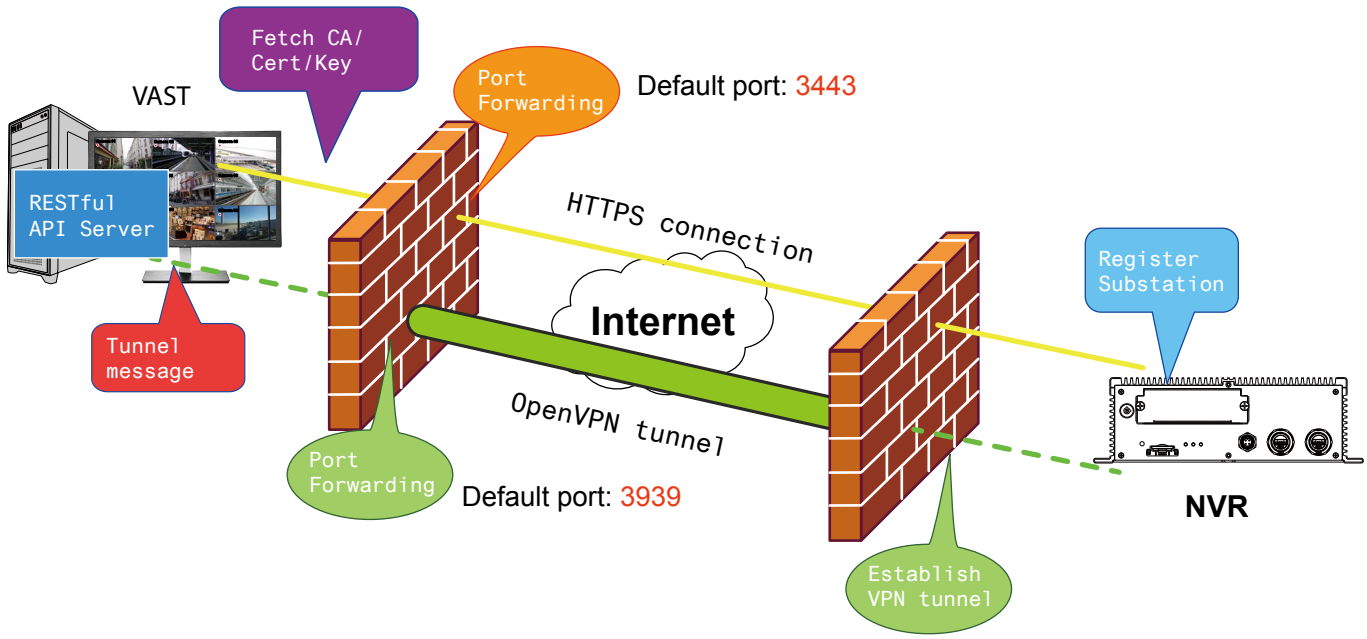
NOTE: 32 camera channels are for free.

Installation Option - OpenVPN

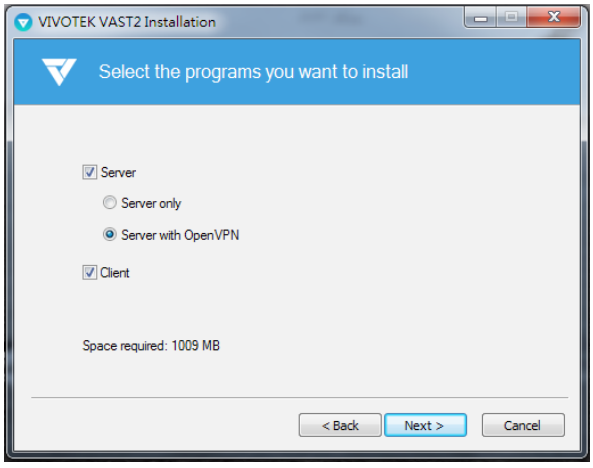
NAT-traversal with OpenVPN

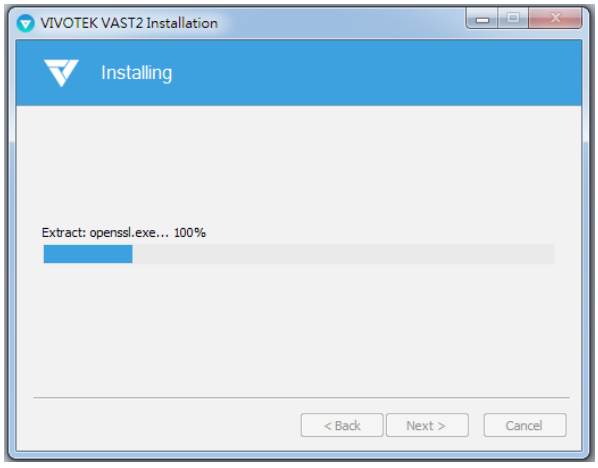
You can select the "VAST Server with OpenVPN" option when installing the VAST server. A remote connection from NVR via a 3G/4G/LTE network can be made through an OpenVPN tunnel. When the OpenVPN option is selected, an OpenVPN server will be installed with the VAST server.

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



The sample installation screens are shown below:





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

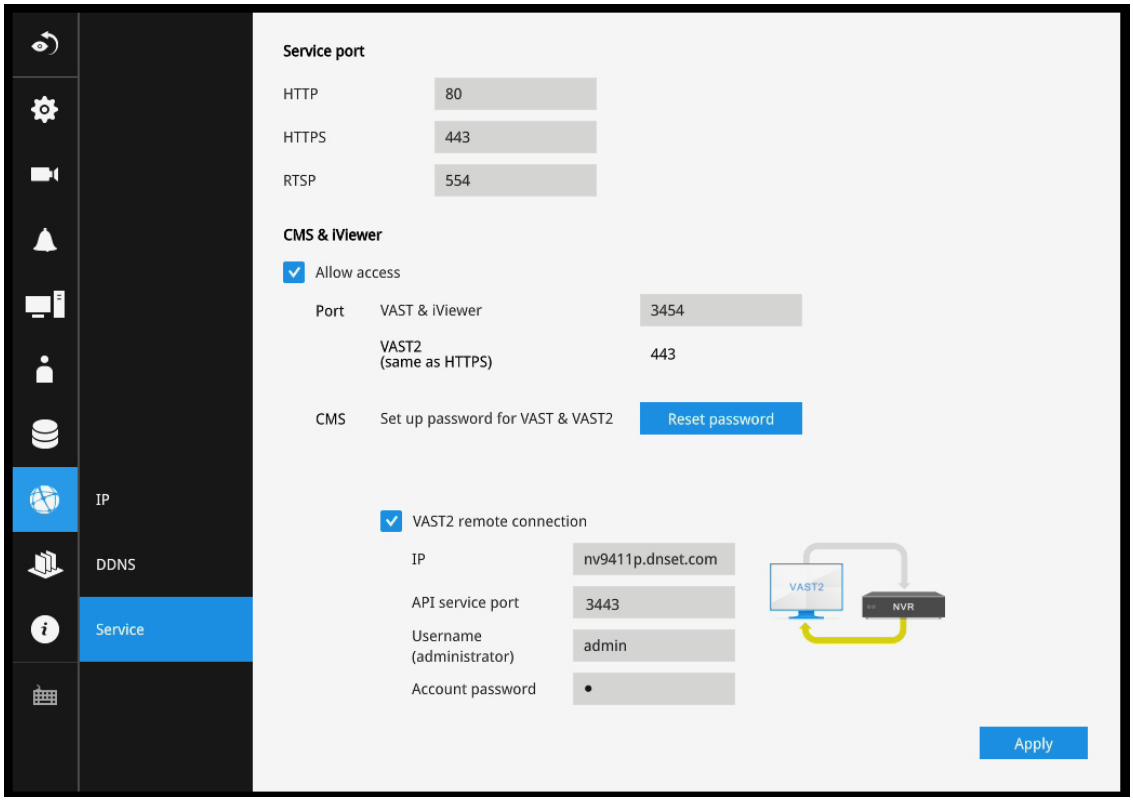
You can edit your VPN IP subnet parameters according to your network configuration. The contents of the editable text file looks like this:

```
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.

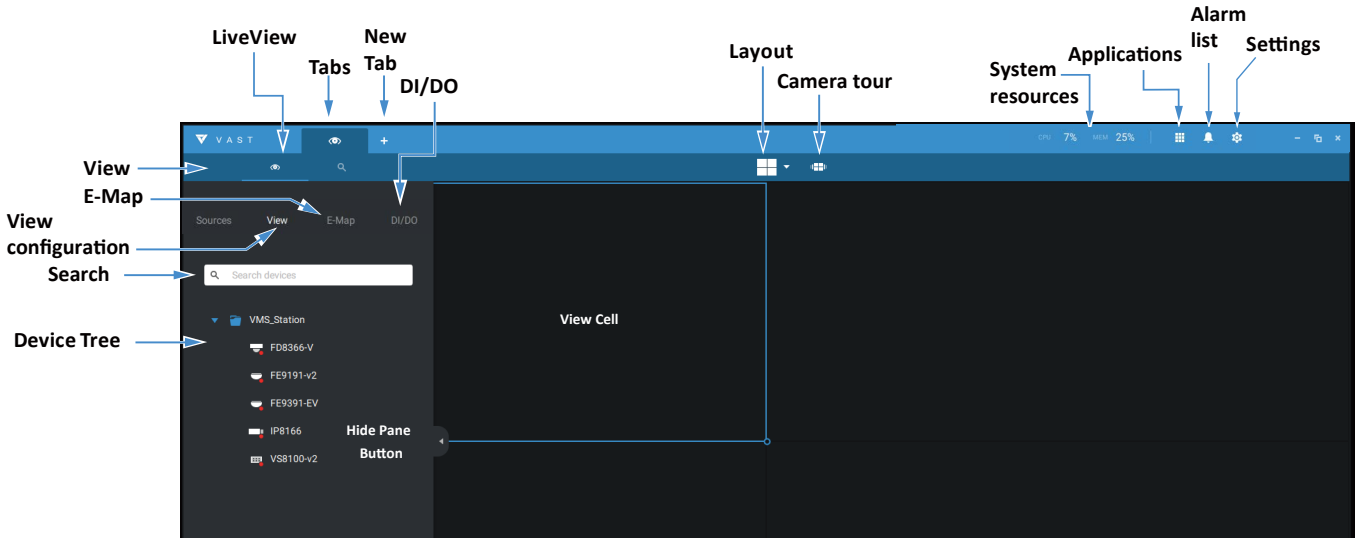
A public IP or domain name must be configured on the VAST server for the access through the Internet. The IP or domain name can contain alpha-numeric characters [0-9][a-z][A-Z][-]. [-] can not be the beginning or the ending character.



Chapter 2-1 Basics: Control and Elements

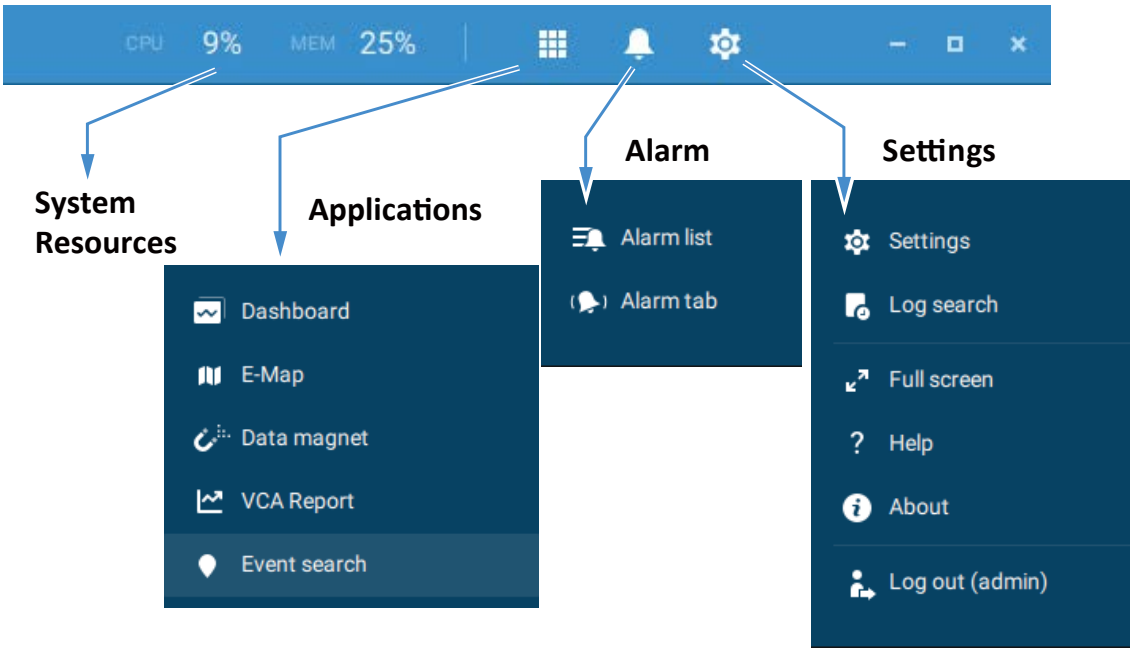
The basic screen elements of VAST live view, playback, and search pane are shown below:

Live view

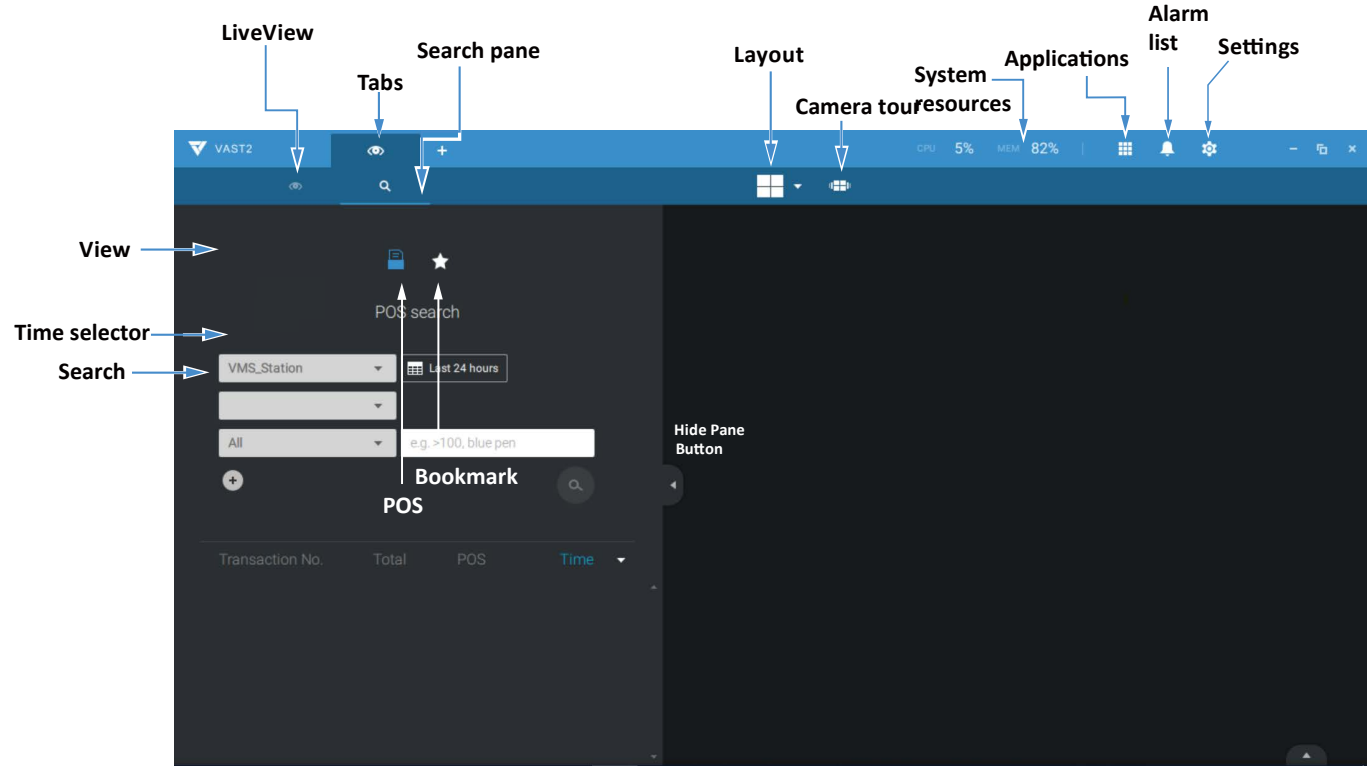


Playback is evoked when a view cell is selected, and you click the Palyback button ▶ on the upper right of the view cell.

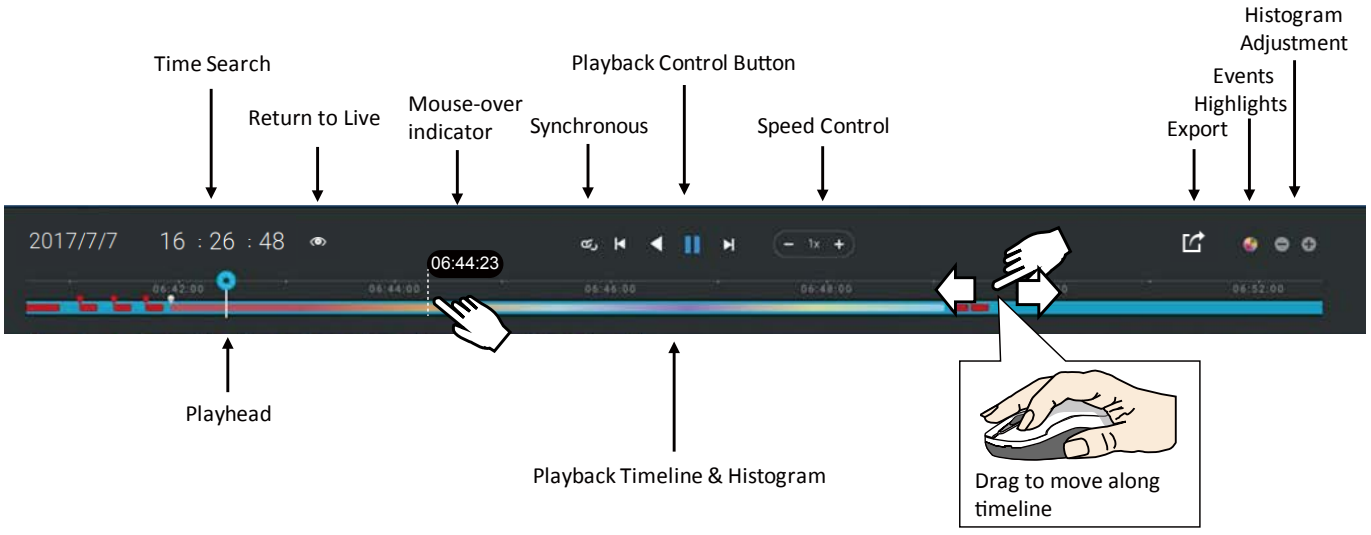
Top Tool Bar



Search Pane

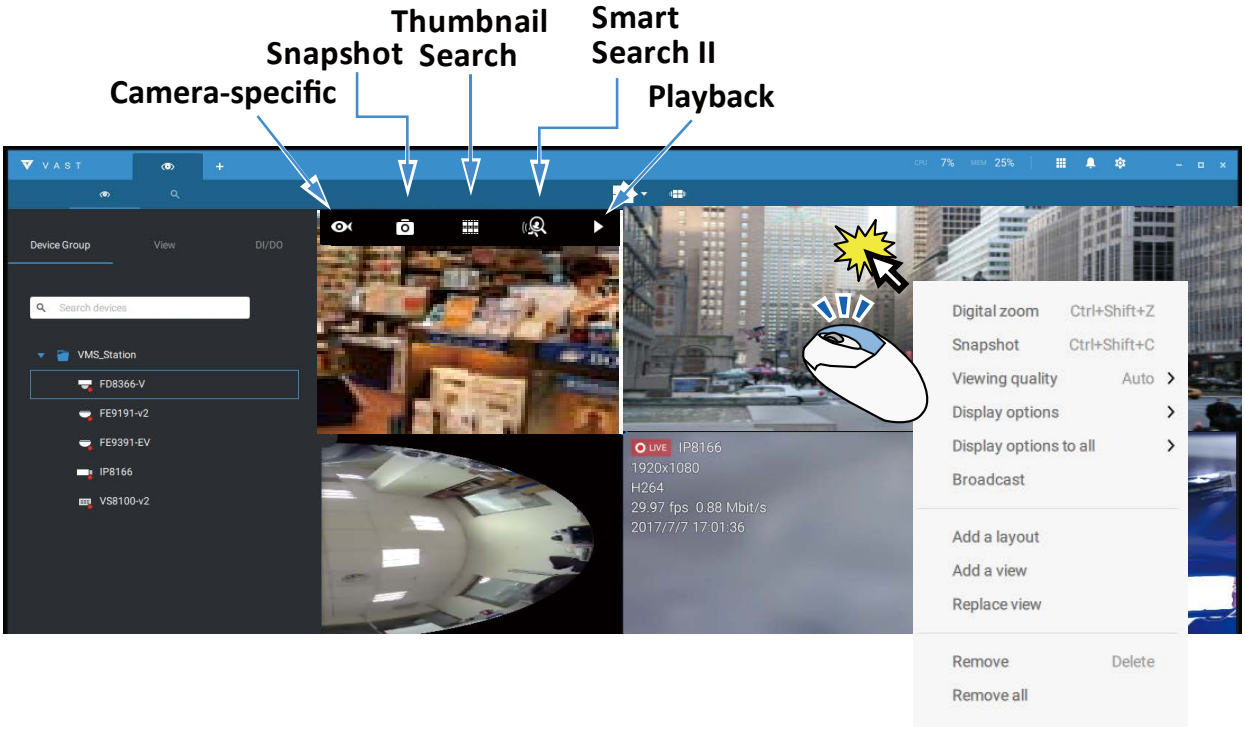


Playback Control



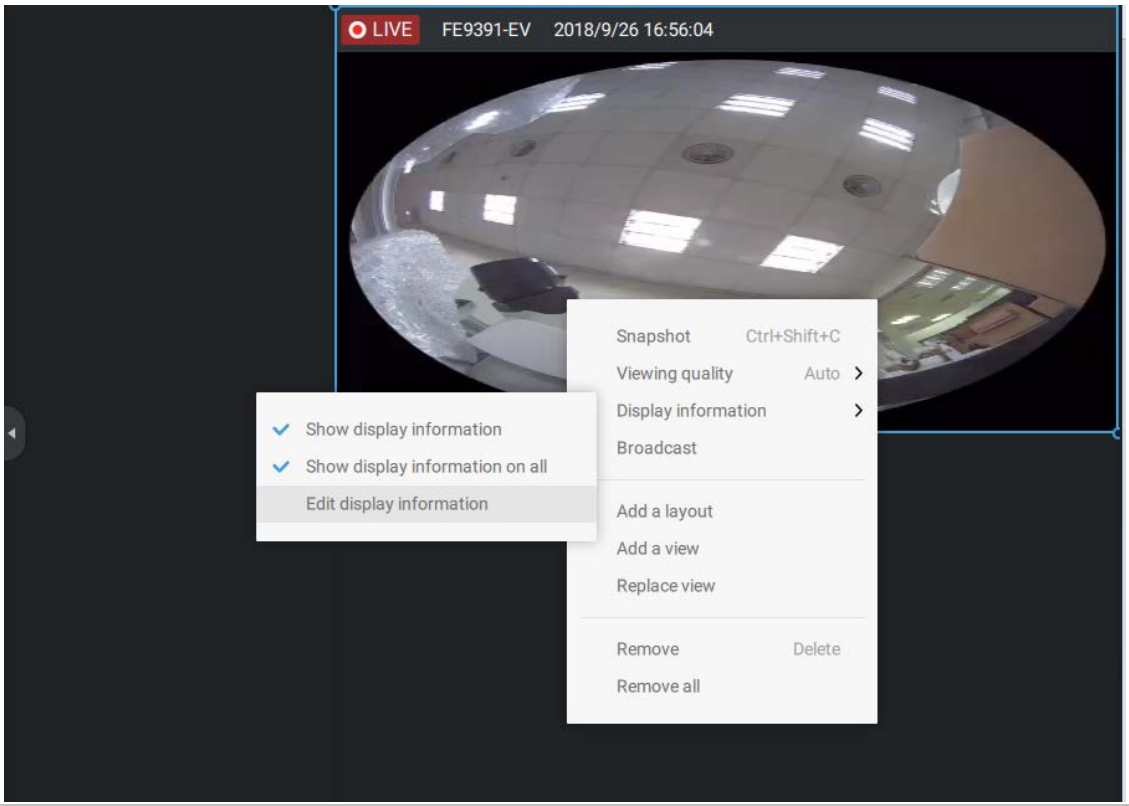
View cell control

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



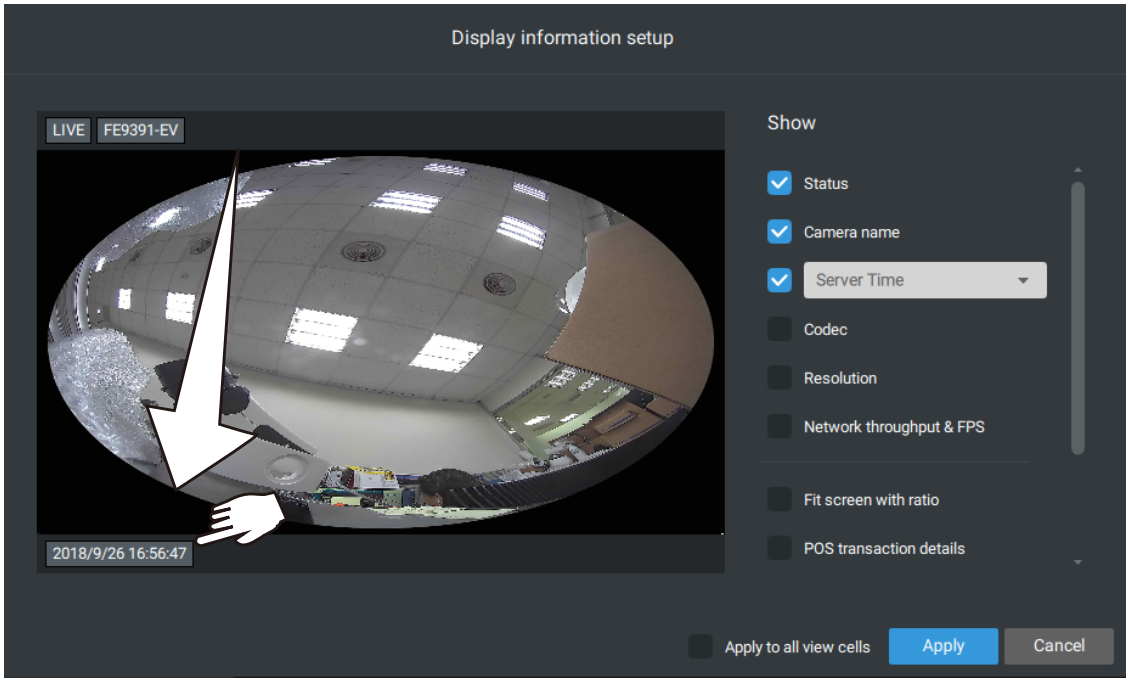
Text overlay

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.

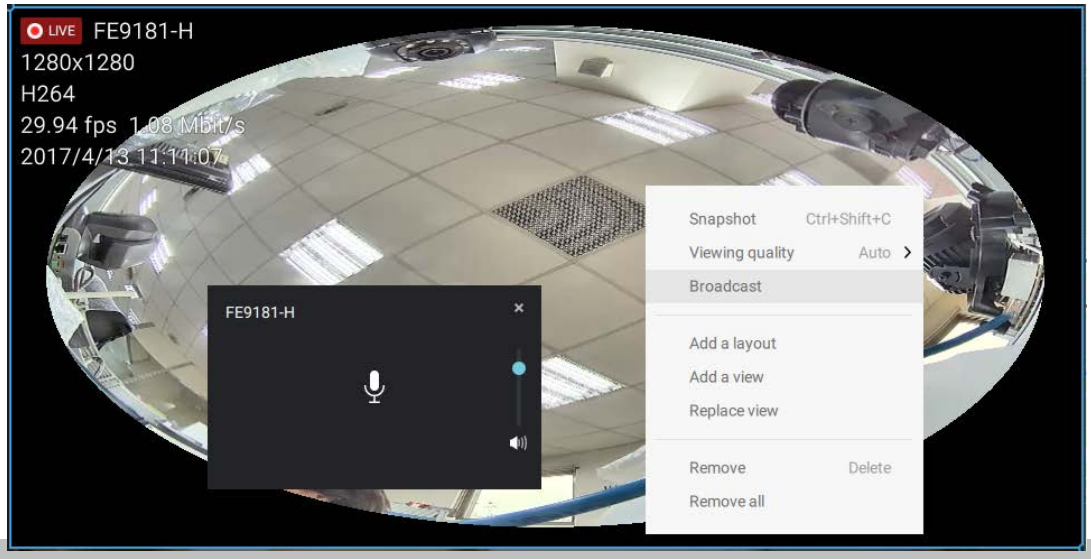
You can apply your current configuration to all view cells by selecting the **Apply to all view cells** checkbox. Note that you can also display the VCA rules and areas on screen.



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.



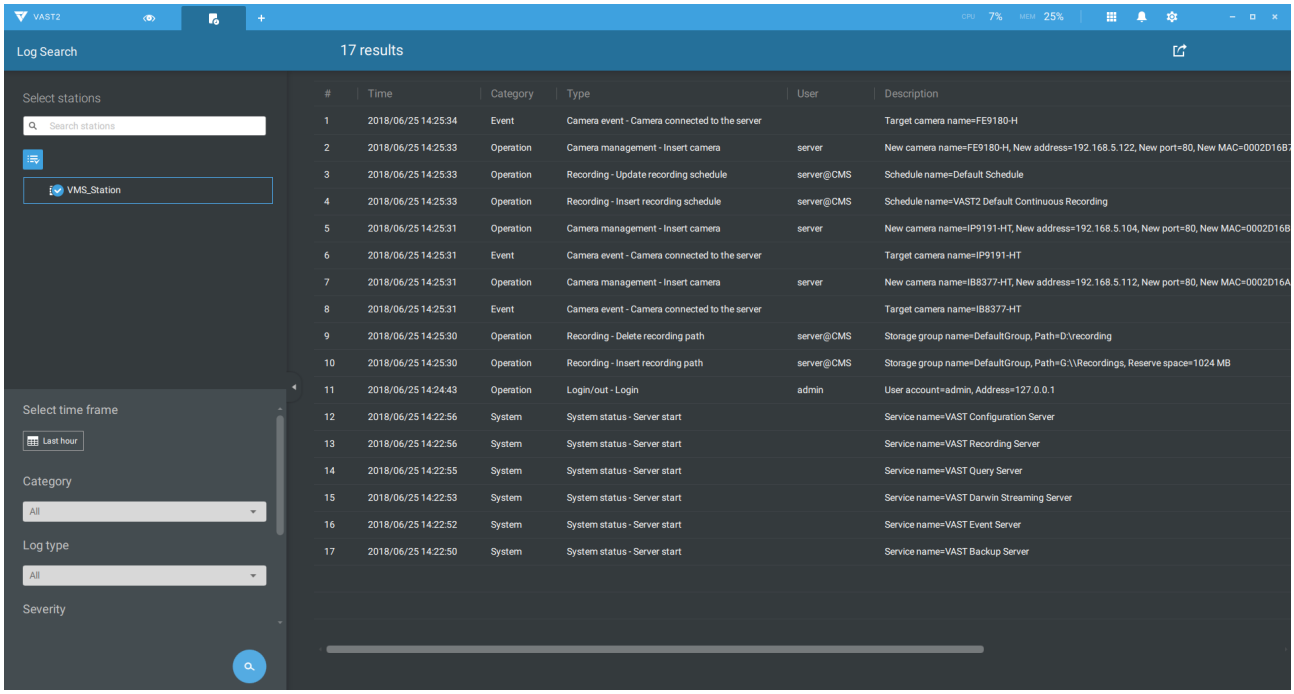
Full Screen

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

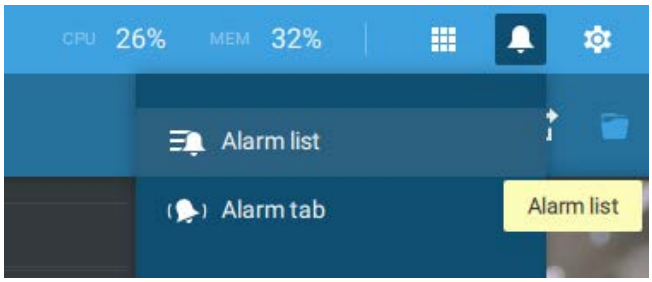
System logs can be found via the tool bar tab. All system events will be listed in the Log search panel. If you have multiple server, substations, select a server. You can search specific events by the event types (All triggers, camera, system/site, external devices), or by the time of occurrence using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

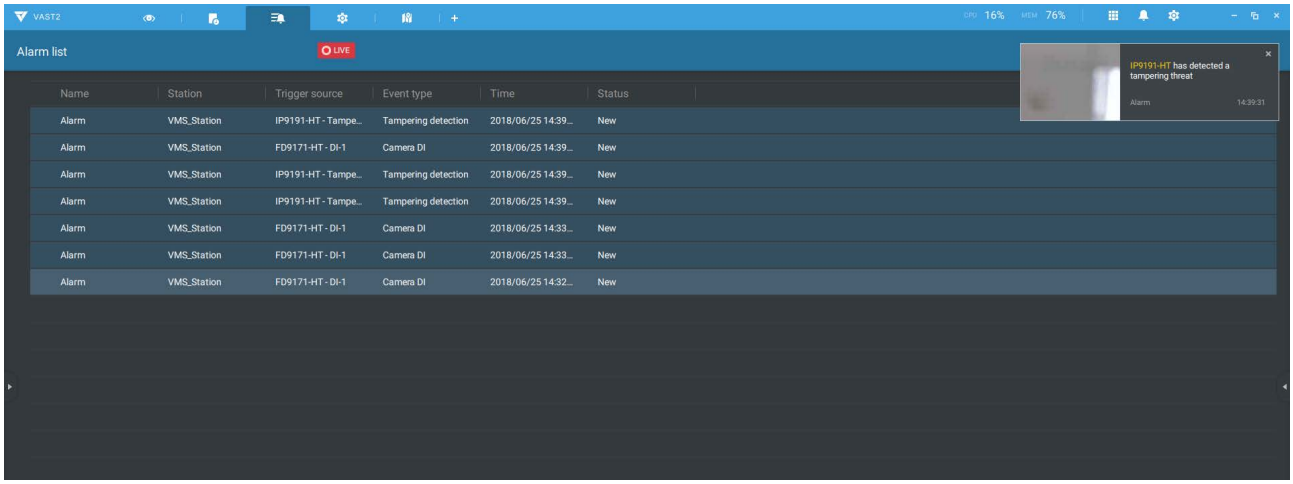
Use the Export button  to export the system log as an individual log file.



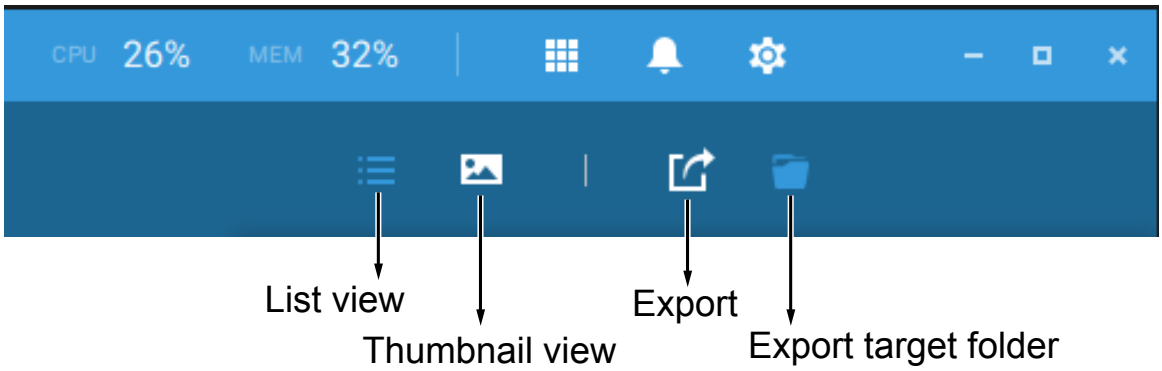
Alarm list

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.

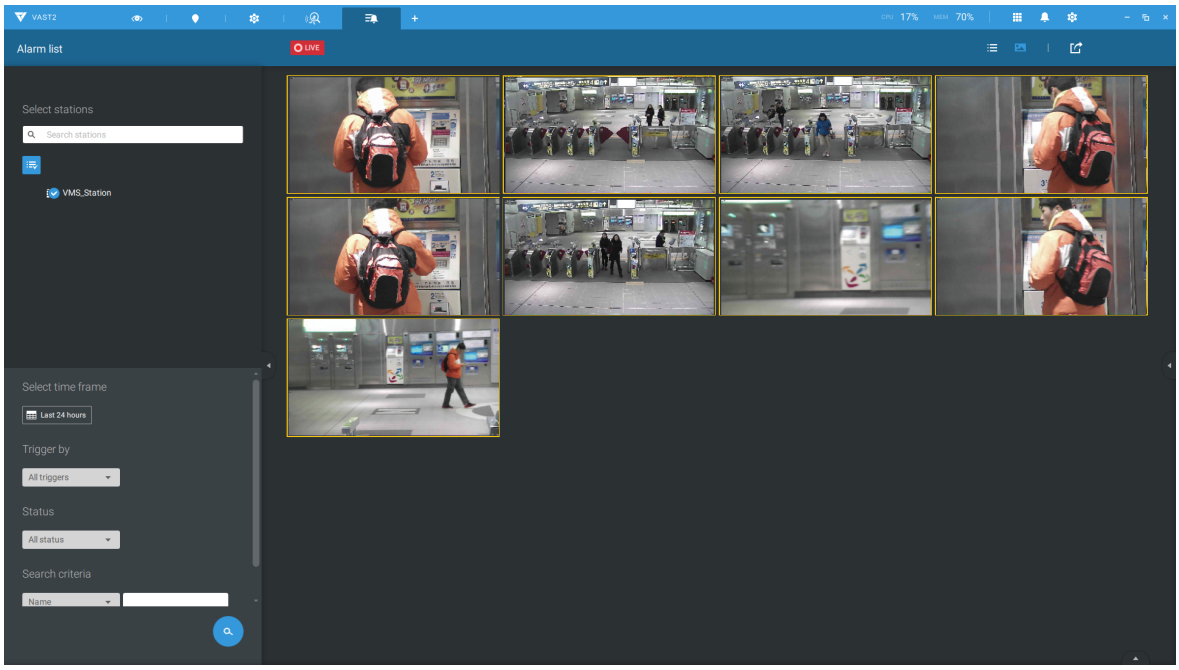




The Alarm list can be displayed in either the List view or Thumbnail view.



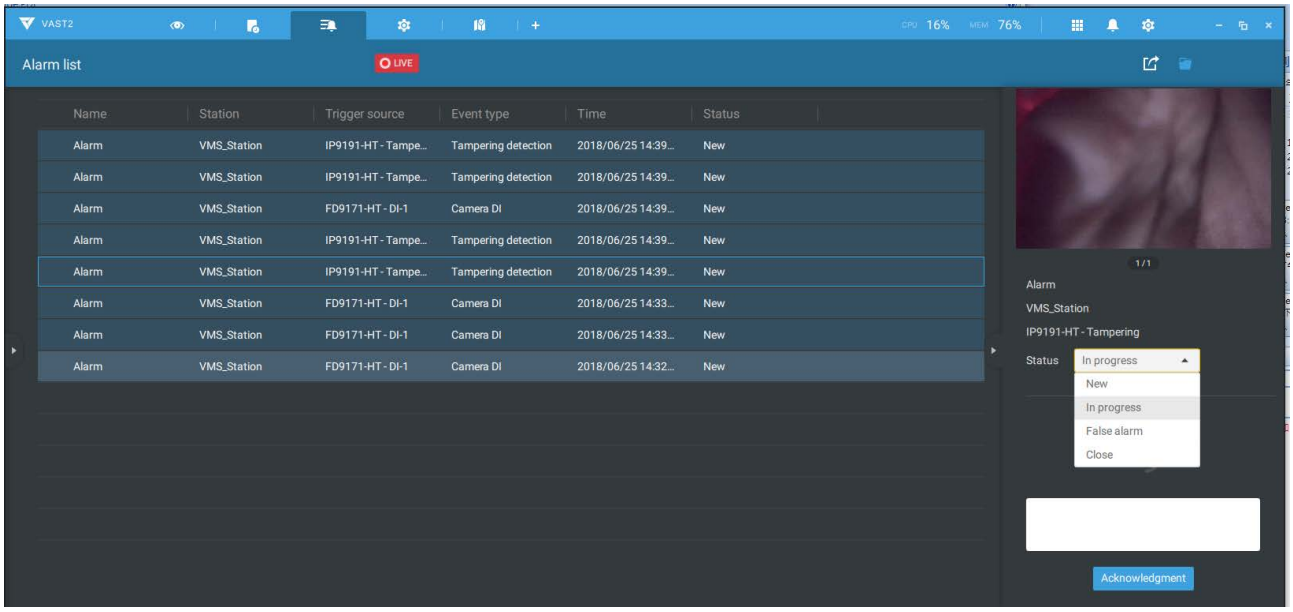
Below is an example of a Thumbnail view.



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.

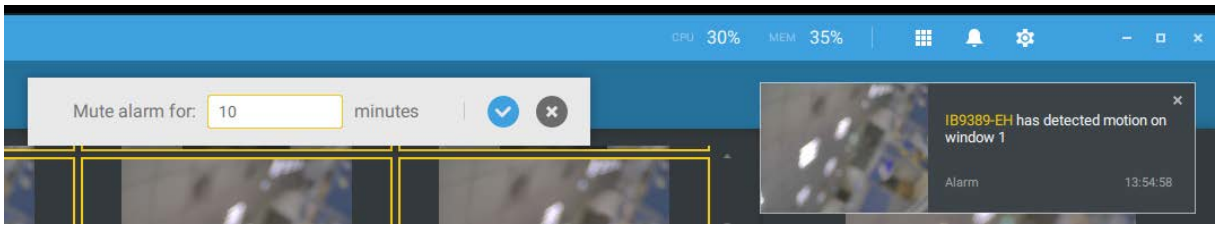
When done with designating event status, click the Acknowledgment button.



The Alarm list also supports Hot keys.

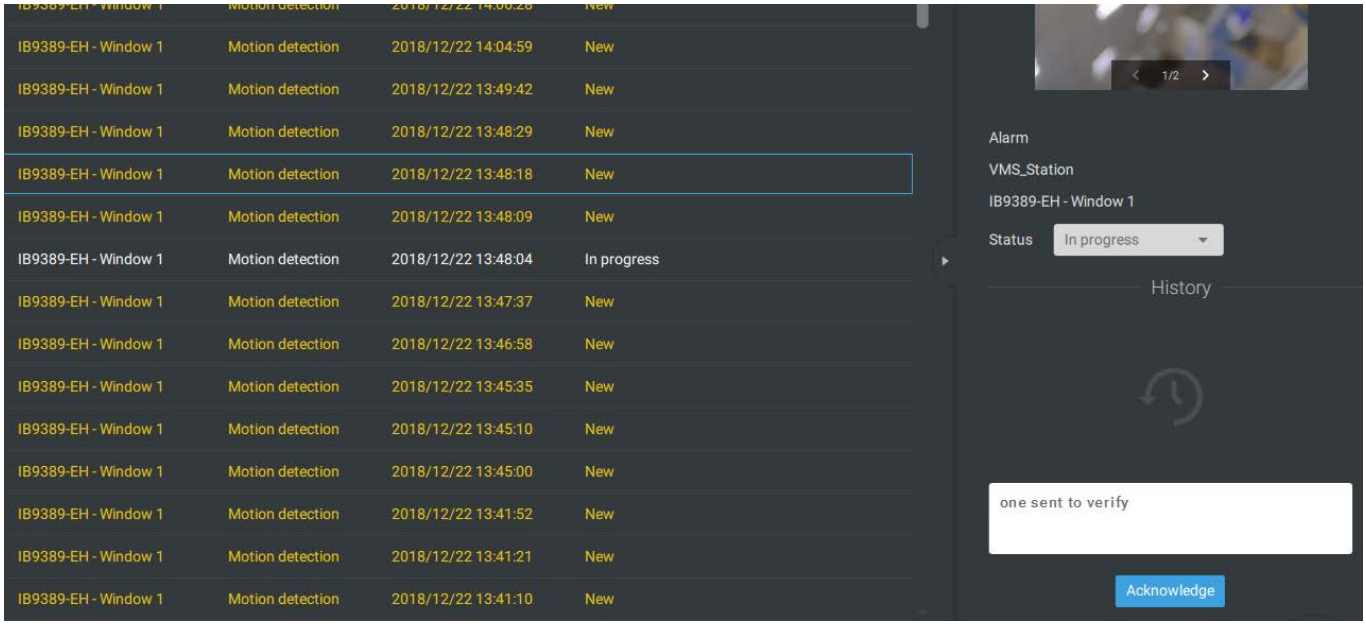
Alarm list window			
Mute the current alarm	Ctrl		m
Designate the selected alarms as false alarms	Ctrl		f
Select all alarms	Ctrl		a
Select one or multiple alarms	Ctrl		left mouse button
Select multiple alarms		Shift	left mouse button
Select different alarms			Up/Down/Left/Right

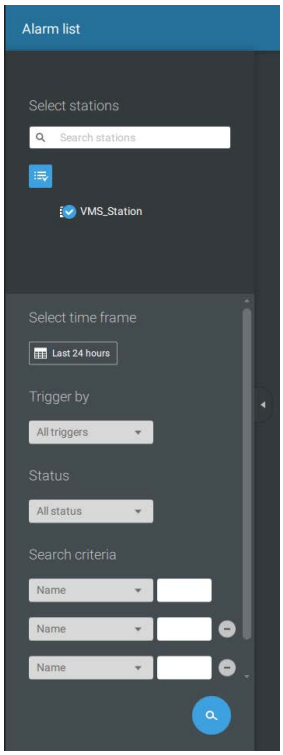
When an alarm is muted, a message will prompt asking for how long the alarm will be muted. Enter a number, and the alarm will disappear from the list temporarily.



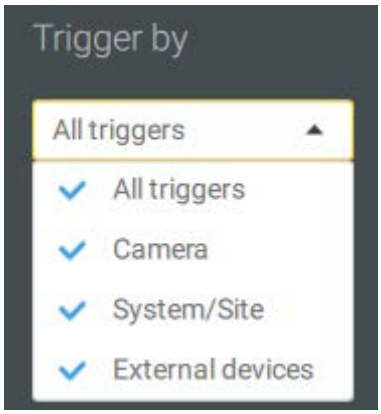
When an alarm is designated as a false alarm, it is immediately removed from the list.

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

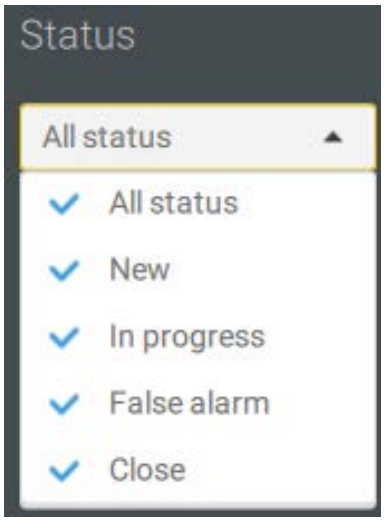




To find alarms of specific types, time of occurrences, and alarm status, click the side tab to reveal the search panel.



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



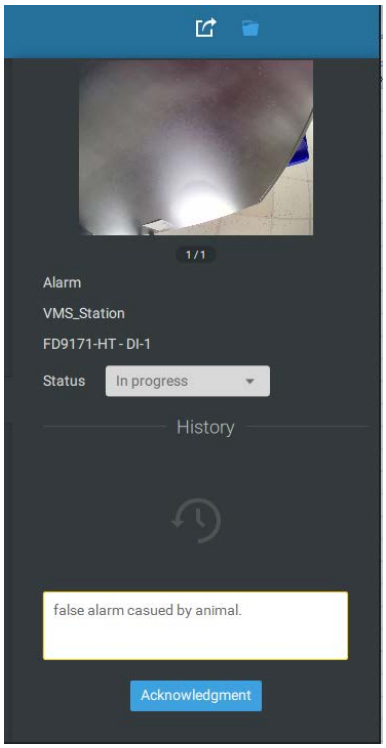
You can check to see alarms of a specific status. For example, you can select to search for the "In progress" alarms only.

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

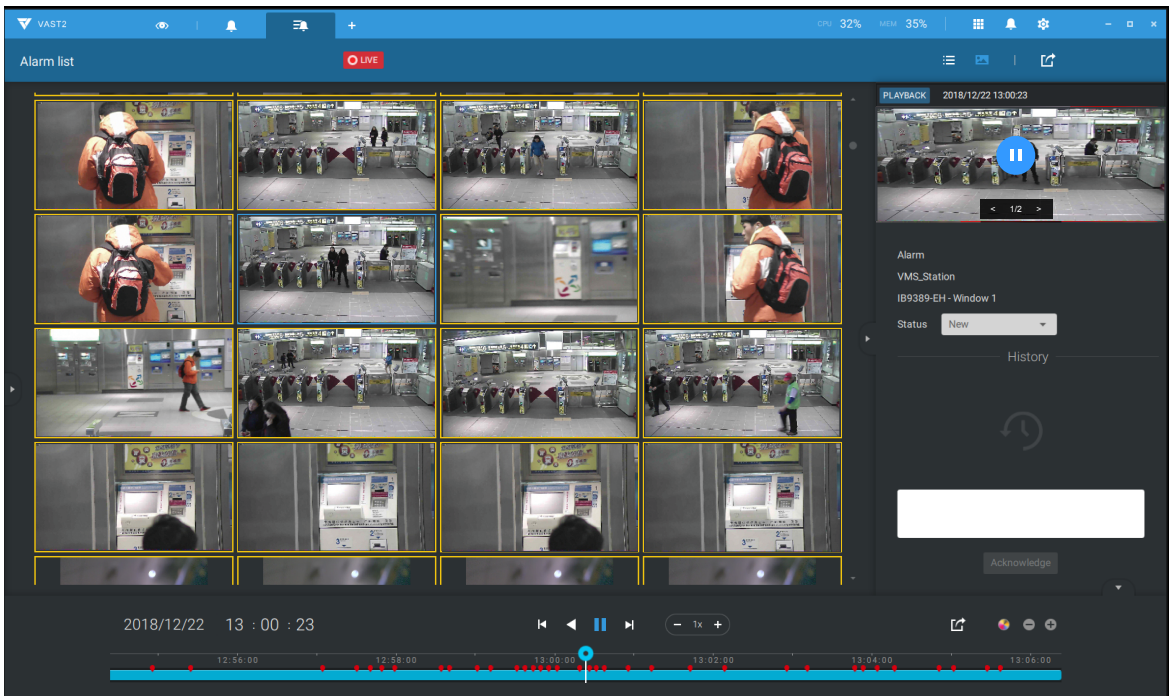
For example, if you have an alarm named as "Alarm3-sidewalk," use the name as the keyword to search for the related alarms.

You can use the Export button to 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.

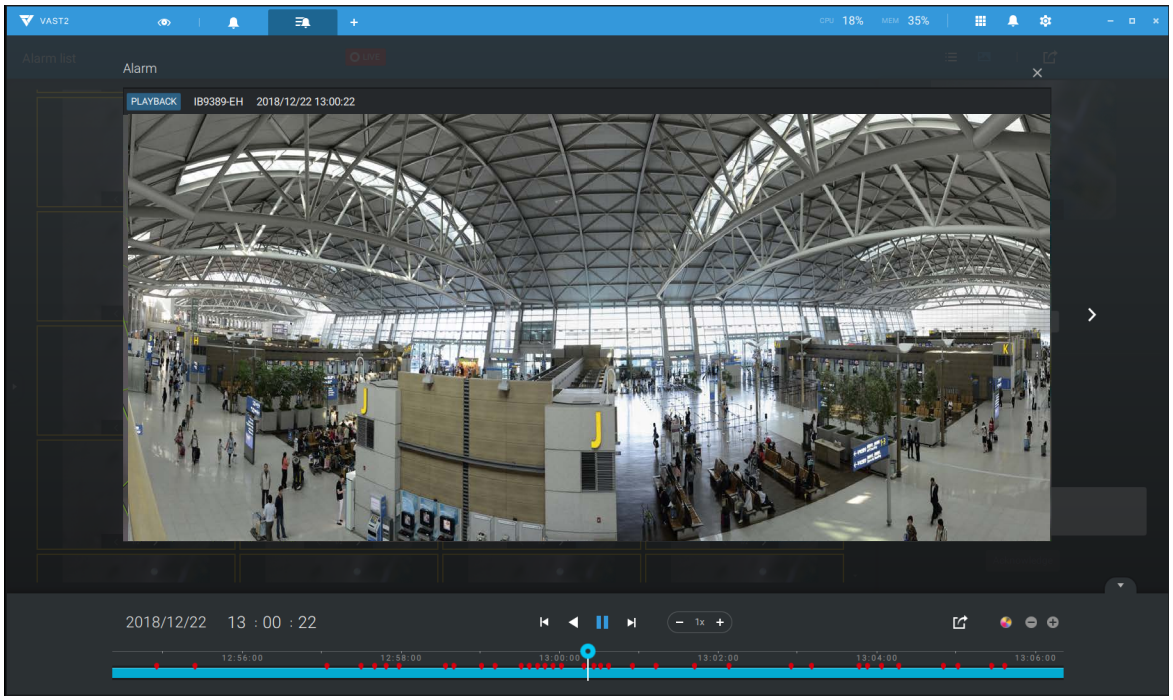
You can also add a comment for an event by entering the description in the comment entry field.



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.

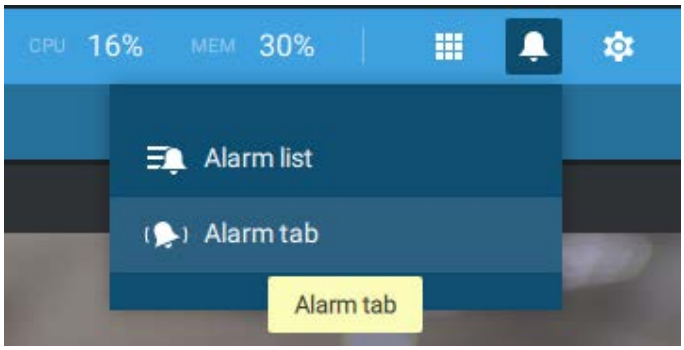


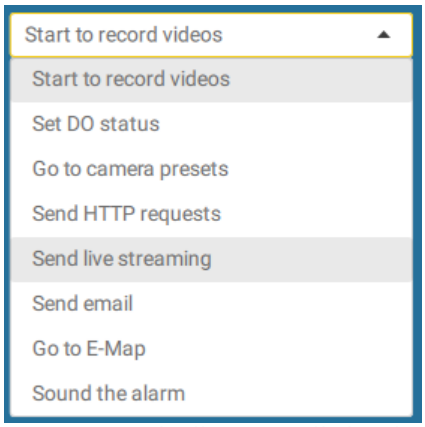
Double-click on the small playback screen again to bring it to the full view. The playback control, time line, export, and alarm tags will be available on screen.



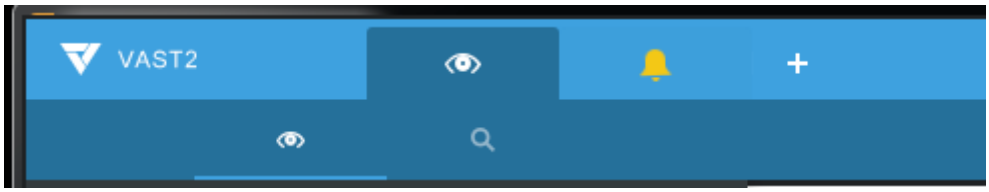
Alarm tab

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.

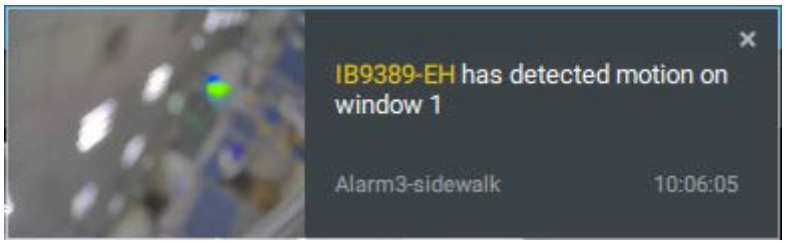




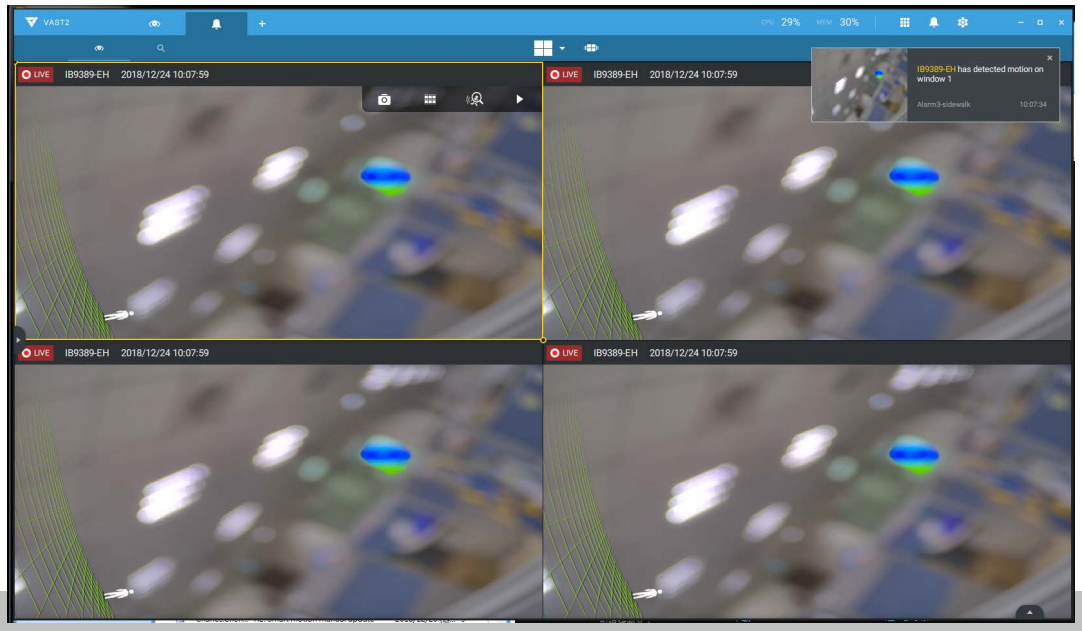
When a live streaming is sent with an alarm, an orange ringing bell icon will display.



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.



Hot Keys

Open online document			F1
Close current tab	Ctrl		W
Full screen	Ctrl	Shift	F
Exit full screen	Ctrl	Shift	F
Exit full screen			Esc
View cell			
Select view cell			Arrow keys
Digital zoom	Ctrl	Shift	Z
Snapshot	Ctrl	Shift	C
Instant bookmark	Ctrl	Shift	B
Remove camera from cell			Del
Move to preset position	Ctrl		Digits (1,2,3,...)
PTZ model up, down, left, right			Arrow keys
Save current layout as a customized layout	Ctrl		S
Undo layout modification	Ctrl		Z
Redo layout modification	Ctrl		Y
Timeline			
Sync Playback mode	Ctrl	Shift	S
Pause (Play/Rewind)			Space
Play	Ctrl		Arrow right
Rewind	Ctrl		Arrow left
Speed up	Ctrl		Up
Speed down	Ctrl		Down
Next frame	Ctrl	Shift	Arrow right
Previous frame	Ctrl	Shift	Arrow left
Reset speed to 1x	Ctrl		1 (one)
Smart search II			
- Configuration page			
Delete detection range			Esc/Del

Bookmark search			
Select more bookmarks	Ctrl		Click
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 device			Del
SMTP Settings			
Remove selected SMTP server			Del
Camera Management			
Rename selected camera			F2
Rename selected folder			F2
Remove selected camera from system			Del
Sites Management			
Rename selected site			F2
Remove selected site from system			Del
Users Settings			
Remove selected user			Del
Schedule Settings			
Remove scheduled time frame			Del

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		m
Designate the selected alarms as false alarms	Ctrl		f
Select all alarms	Ctrl		a
Select one or multiple alarms	Ctrl		left mouse button
Select multiple alarms		Shift	left mouse button
Select different alarms			Up/Down/Left/Right

For a client running on MAC:

Full screen	Command ⌘	Shift	F
Exit full screen	Command ⌘	Shift	F
Exit full screen			Esc

View cell			
Select view cell			Arrow keys
Digital zoom	Command ⌘	Shift	Z
Snapshot	Command ⌘	Shift	C
Instant bookmark	Command ⌘	Shift	B
Remove camera from cell			Delete
Timeline			
Sync Playback mode	Command ⌘	Shift	S
Play/Pause			Space
Rewind/Pause			Space
Play	Command ⌘		Arrow right
Rewind	Command ⌘		Arrow left
Speed up	Command ⌘		Up
Speed down	Command ⌘		Down
Smart search			
- Configuration page			
Delete detection range			Esc/Del
- Result page			
Back to result page			Esc
Next result			Arrow right
Previous result			Arrow left

Data Magnet			
Search result table			
Next result			Arrow down
Previous result			Arrow up
Play selected result			Enter

License management				
Show/hide the entry in online license management	Command ⌘	Shift	Option (or Alt)	V
Purchase license table				
Switch between license status and amount of license	Command ⌘	Shift	Option (or Alt)	L

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.

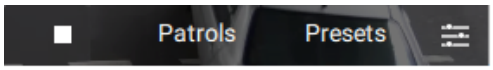
2. **Fisheye** cameras:  Fisheye display mode - Snapshot - Thumbnail search - Smart search - Replay.

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.

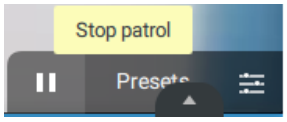
3. **PTZ** cameras:  PTZ - Snapshot - Thumbnail search - Smart search - Replay. For information about PTZ control, refer to the discussion on PTZ on page 99.

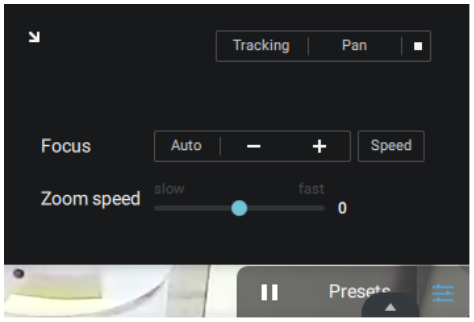
To exert PTZ control, first click on this button  to enable PTZ control.

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

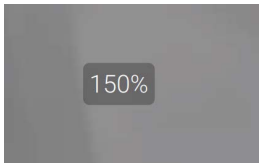


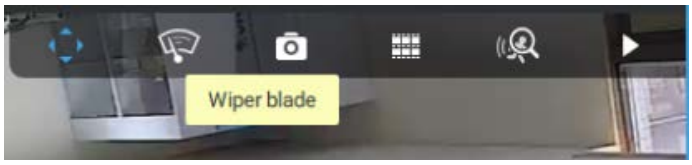
Click Patrols or Presets if these have been configured on the PTZ camera. You will need to open a web console with the camera to do so.





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.

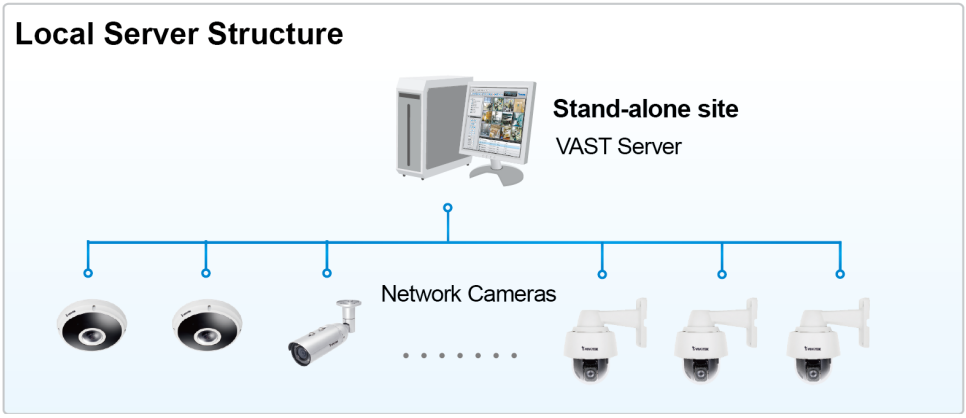
You can use the mouse wheel to zoom in or zoom out on the screen. The zoom ratio is shown on screen for half a second.

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.

VAST Server and Client Components

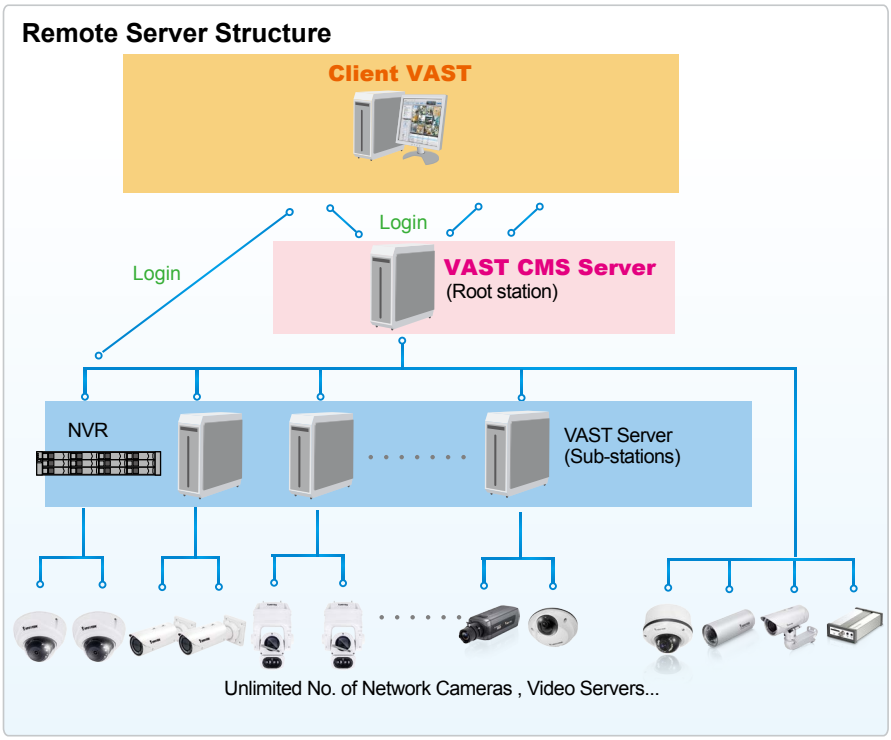
VAST2 Server provides a centralized management site for video recording. Users can login and modify the server's configuration, edit the server's recording storage, configure schedules and many other functions. You can browse the recorded video database and video clips related to specific events on the 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 sub-stations 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, Windows Server 2012, 2016		
Server (Recording Channels)	Up to 64 CH	Up to 128 CH	Up to 256 CH
CPU	6th Generation Intel® Core™ i3 Processors or above		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 recommended***		

* 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 Mojave 10.14		
Clients (Display Channels)	720P,2Mbps, H.264,* each CH	8 CH	16 CH	32 CH
	1080P,4Mbps, H.264**, each CH	6 CH	10 CH	18 CH
	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 Interface Card		Ethernet, 1Gbit recommended		
Graphics Card****		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 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 on the desktop to start the VAST2 main page.

When started the first time, the server automaticallly 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).

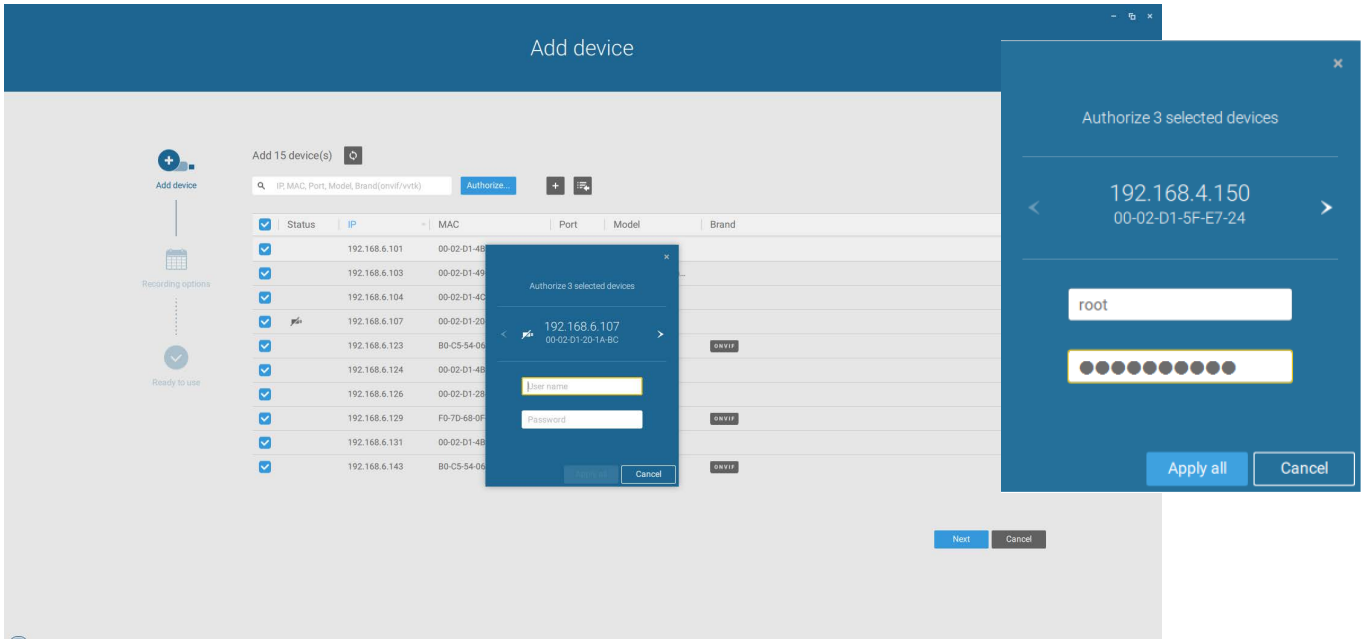
Use the Add device button to manually add a camera with its known IP or domain name.

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.



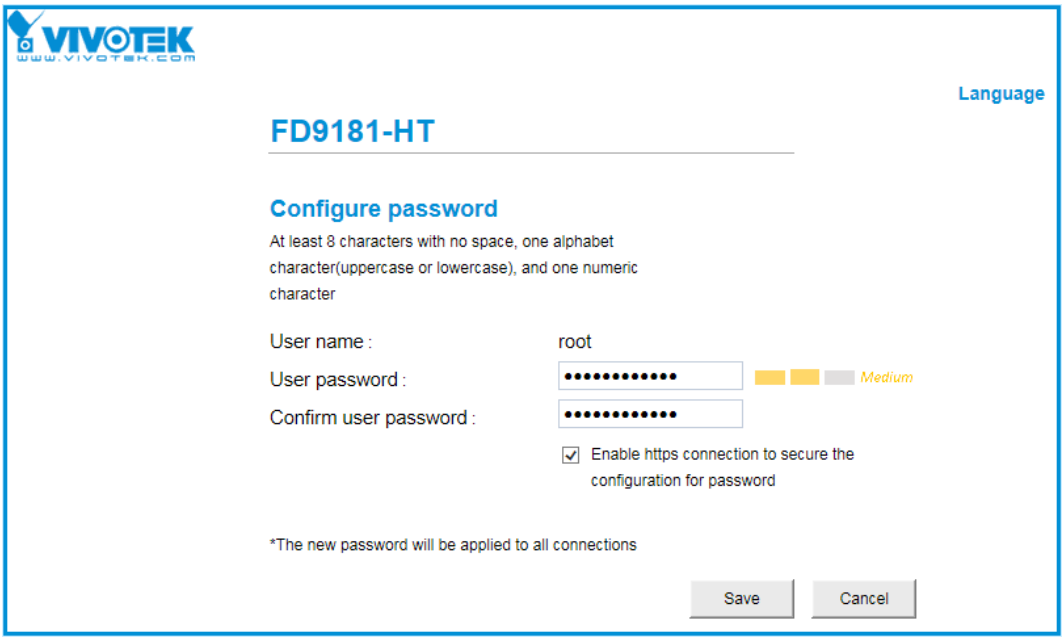
2-2-1. Selecting Devices

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:

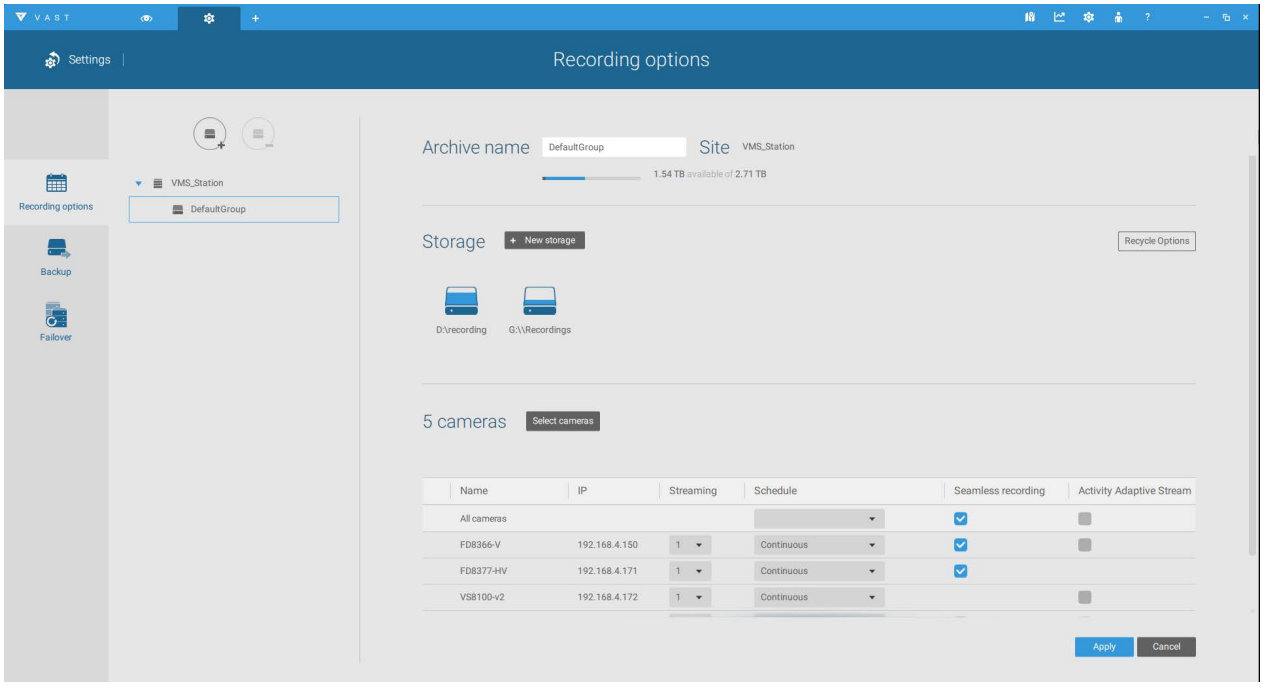
For cameras that come without a password protection, you should open the Shepherd utility to locate and open a web console, and configure a password for protecting the access to the camera. If a brand new camera (with no password) is selected for your VAST configuration, it will join your configuration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



2-2-2. Recording Options

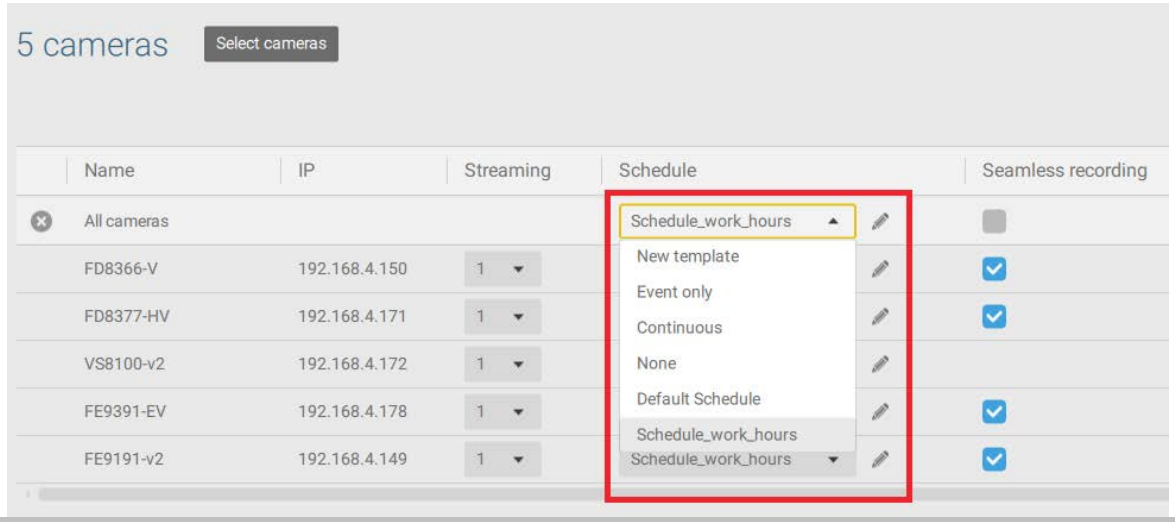
Click Settings > Recording > Recording options. The Recording options window will prompt.

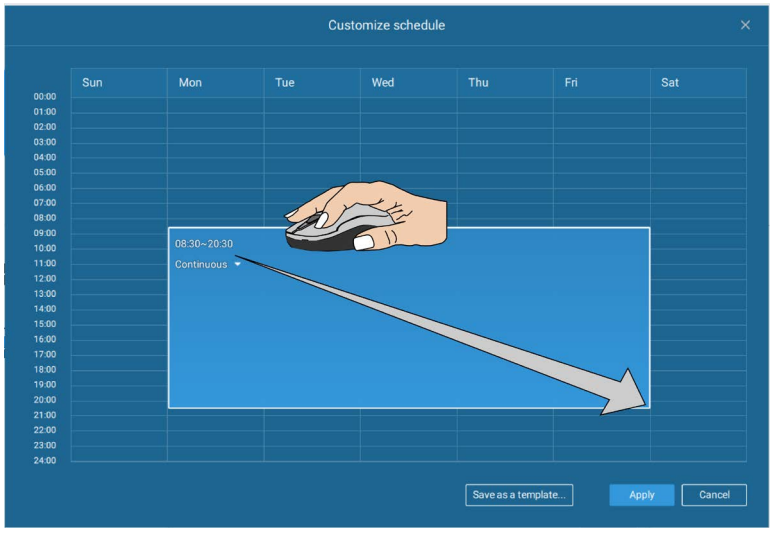
You can configure recording schedules or select the storage options, including the configuration of an external NAS storage.



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 button.

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



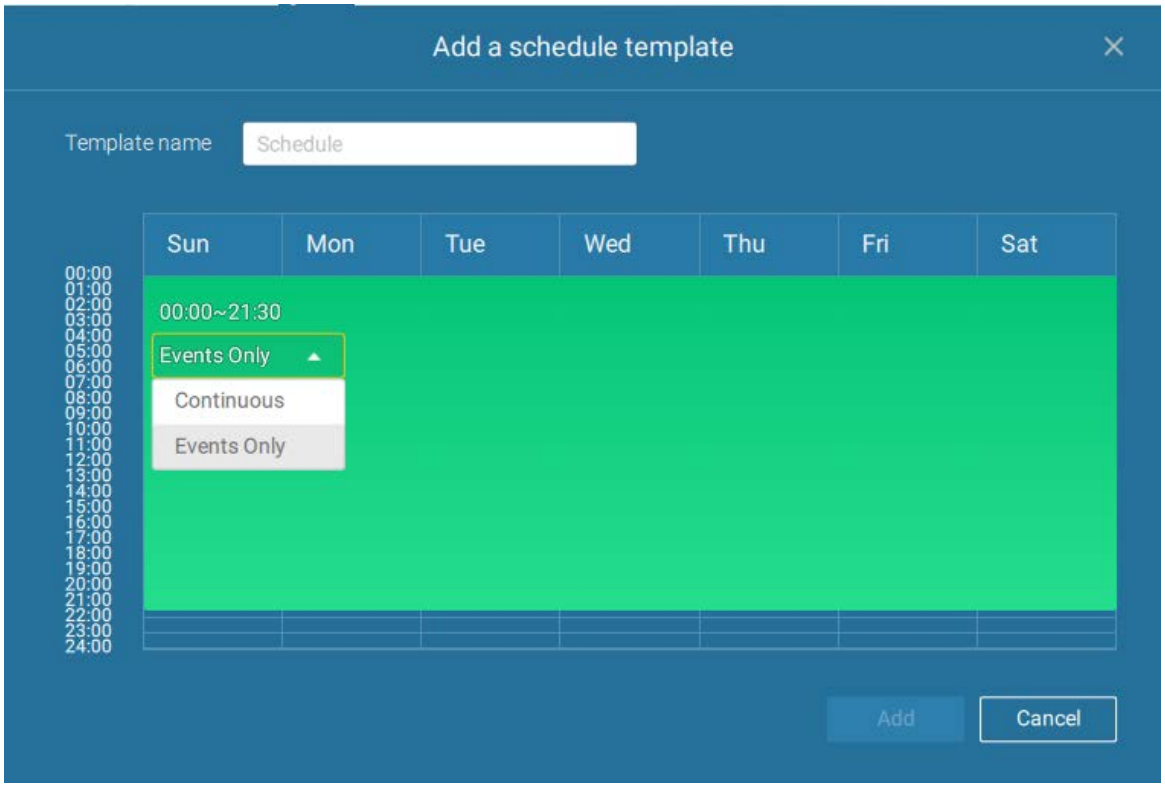


Click and hold down on the time cells, and drag the mouse to include the time span of your preferrence. The minimum selectable unit is half an hour. You can select separate and multiple time spans on the template.

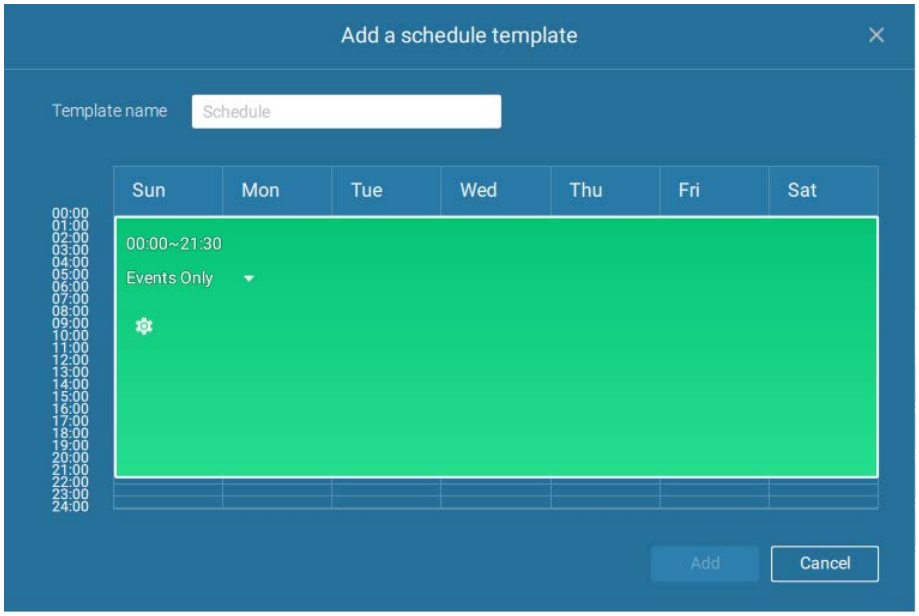
Enter a name for the template, and click Add to save your template.

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

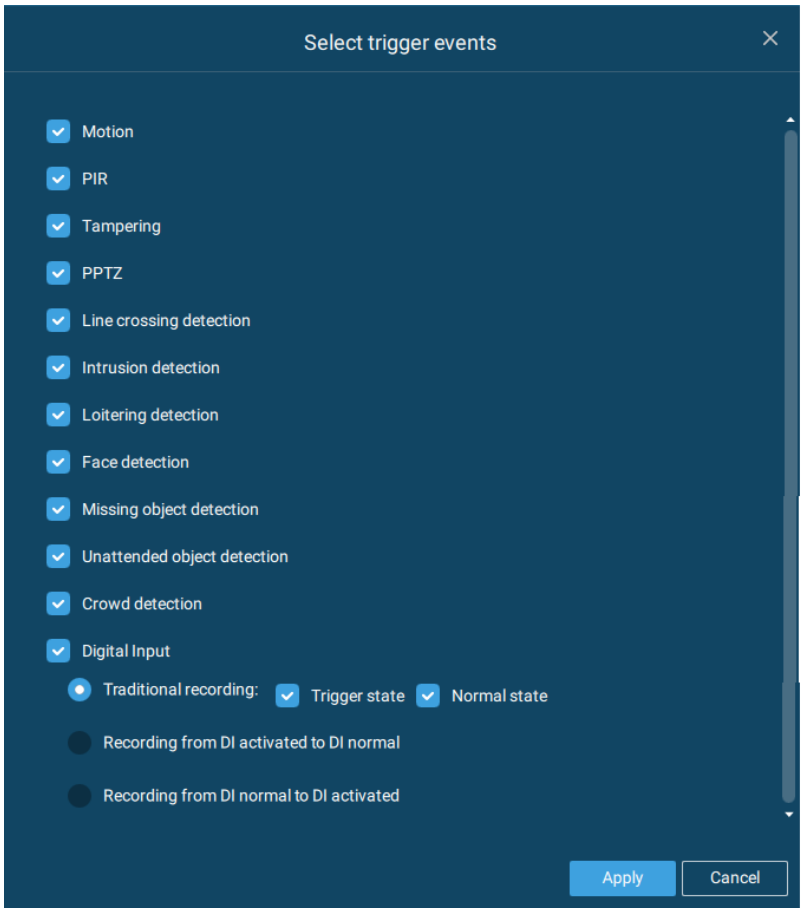
If the **Events only** option is selected for the new template, you can determine what kinds of events will trigger the recording. Use the pull-down menu to select Events only.



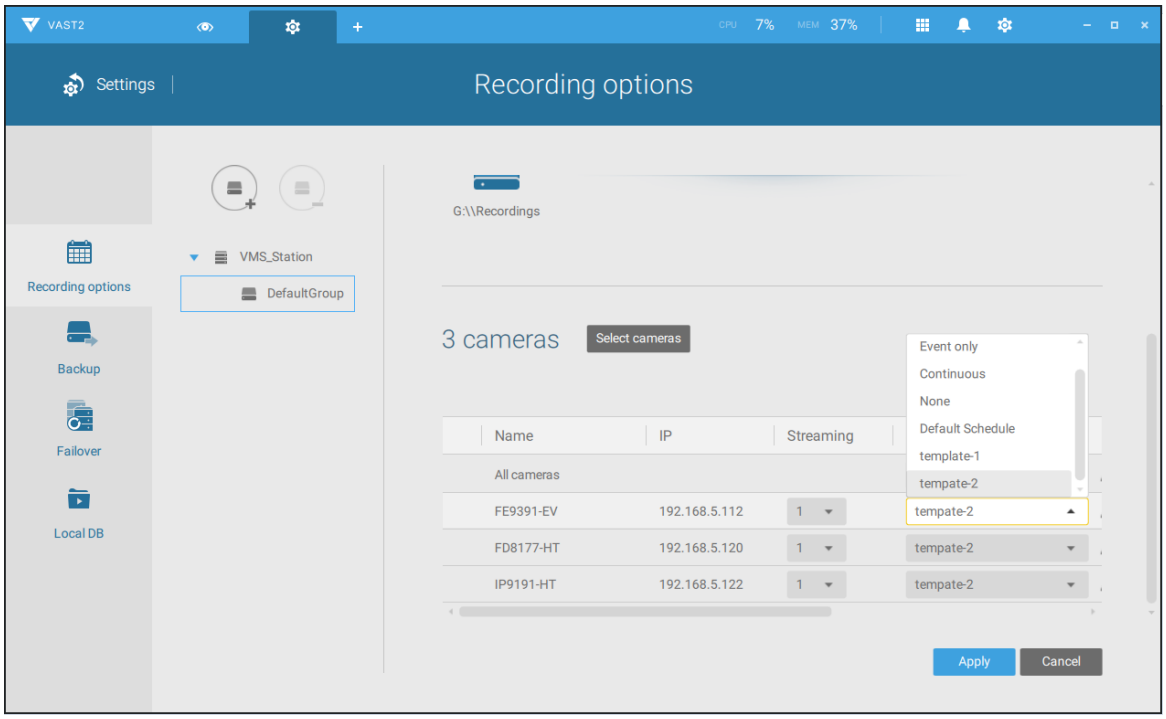
When Events only is select, click on the Settings button to proceed.



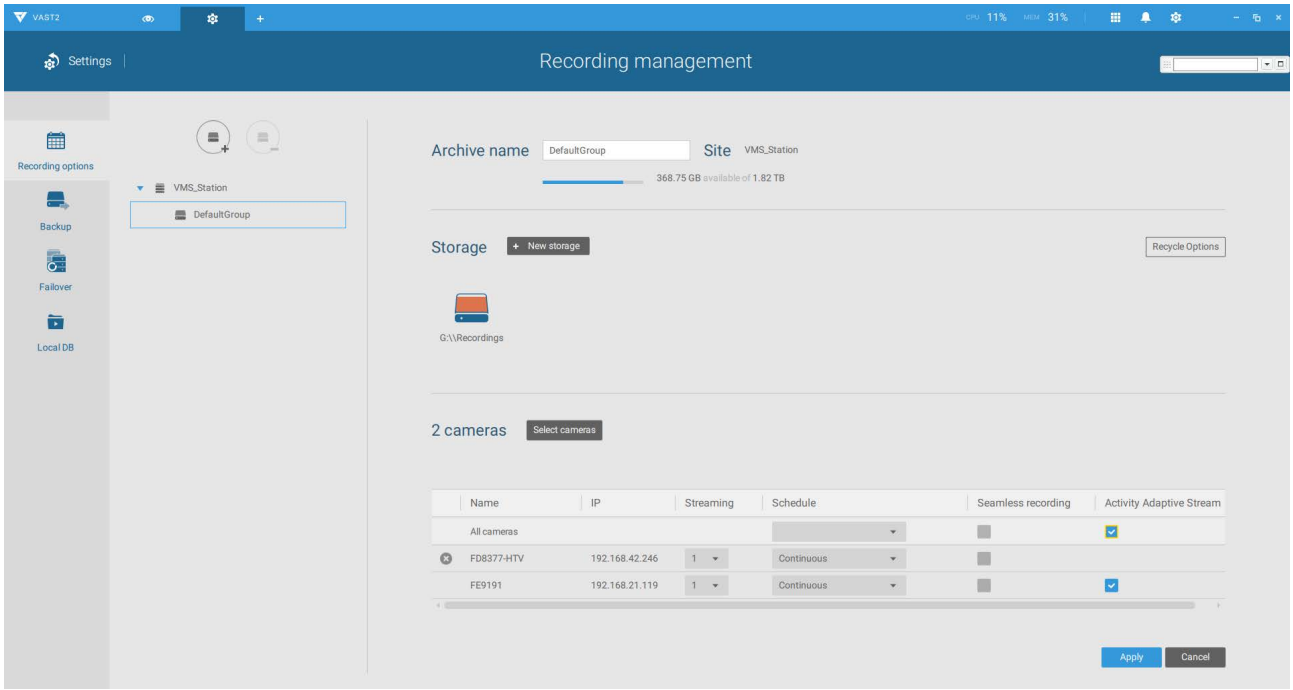
The applicable event types will be listed. Select the types of event triggers that you prefer. Click **Apply** to leave this page. By deault, all applicable event triggers will be selected.



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.



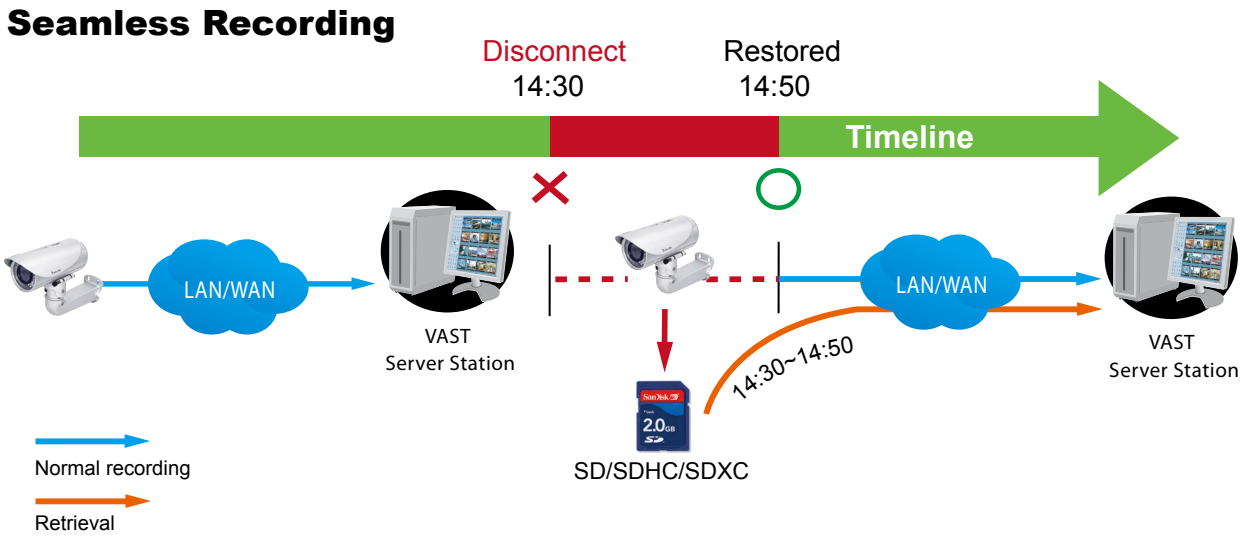
Make sure a Schedule mode is selected when you leave this configuration step.



Seamless Recording

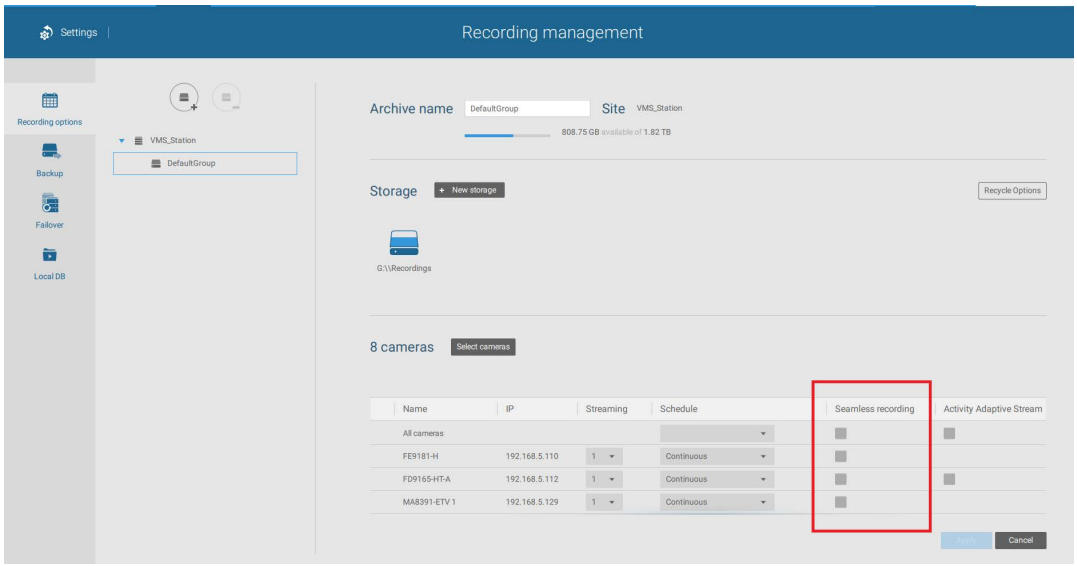
Seamless Recording safeguards critical videos in the occurences of network disconnection.

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/hadware 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.



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 106.

On individual cameras, you can configure the following:

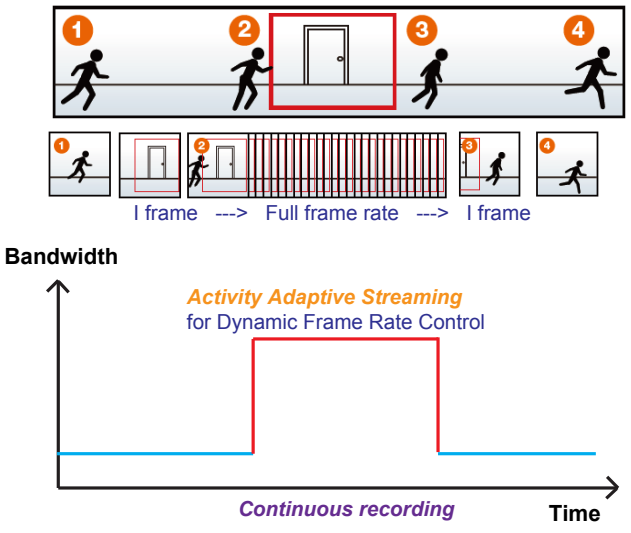
■ Pre-event recording and post-event recording
The Network Camera has a buffer that temporarily holds data for a period of time. Therefore, when an event occurs, the camera can restrieve image frames taken several seconds ago. Enter a number to define the duration of recording before and after a trigger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

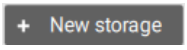
NOTE:

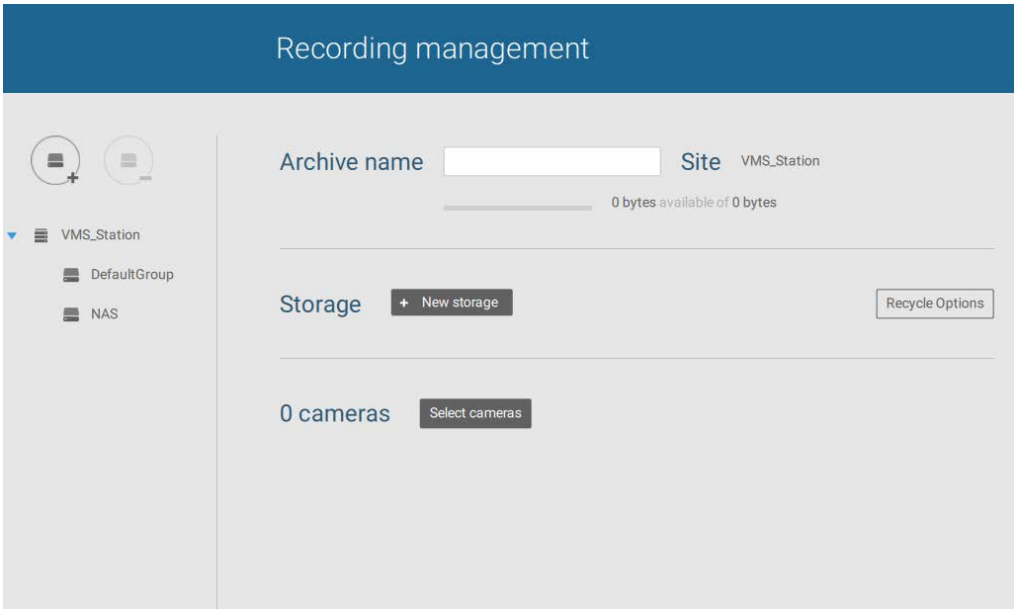
* To enable adaptive recording, please make sure you have configured the trigger sources such as Motion Detection, DI input, or Manual trigger.
* When there is no alarm trigger:
  - JPEG mode: record 1 frame per second.
  - H.264 mode: record the I frame only.
* When the I frame period is > 1 second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



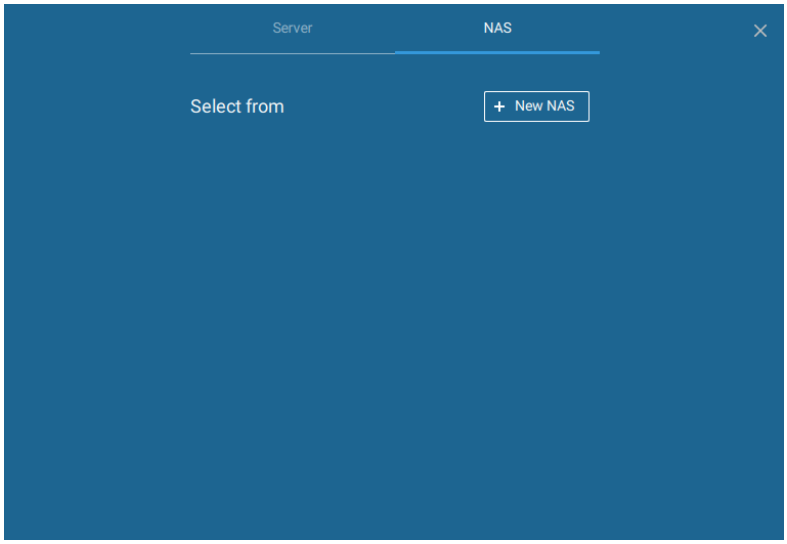
Adding NAS (Network Attached Storage) as a Storage Option

You can also record videos to a networked storage.

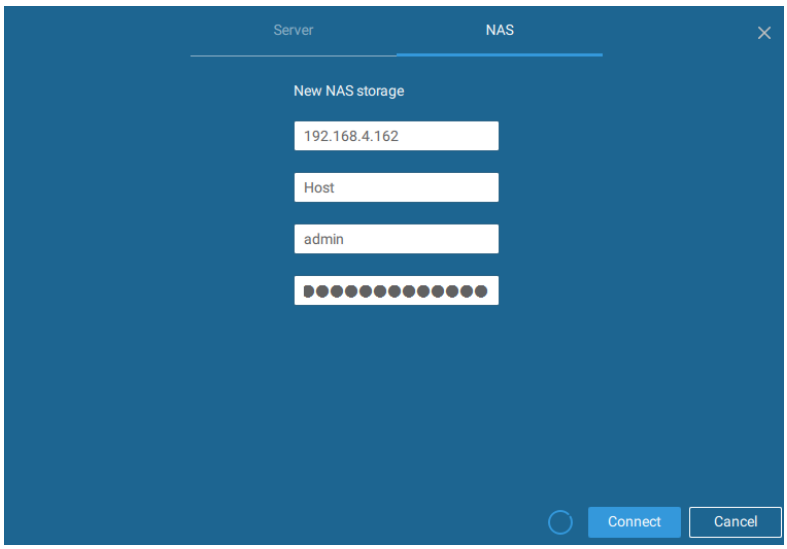
1. Click the Add archive  button.
2. Enter a name for the configuration.
3. Click the Add storage  button.



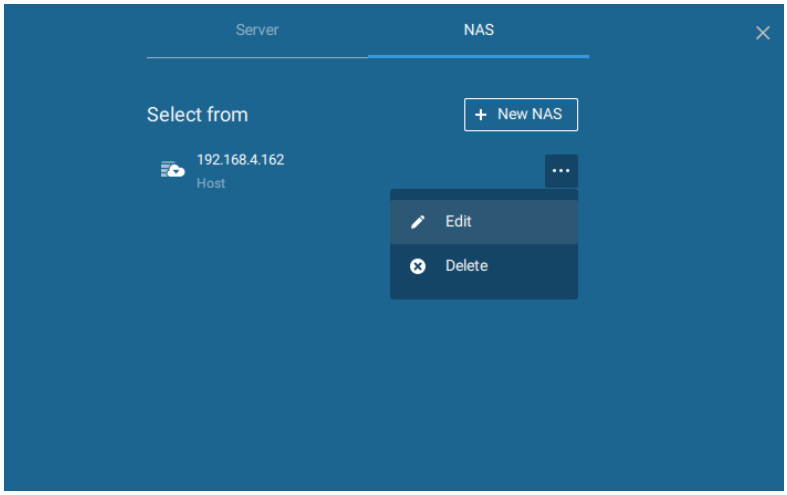
4. Click the + New NAS button.



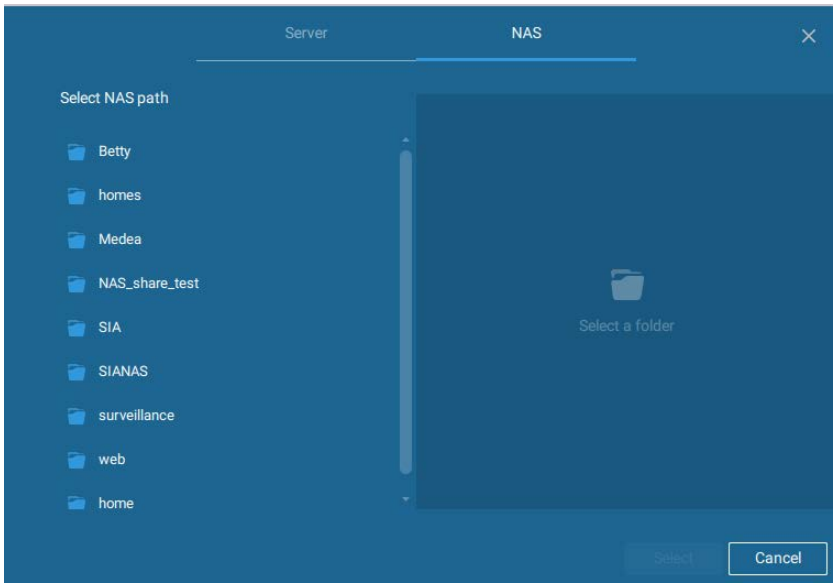
5. Enter the NAS storage's address and the credentials for access to the networked storage. When done, click the **Connect** button.



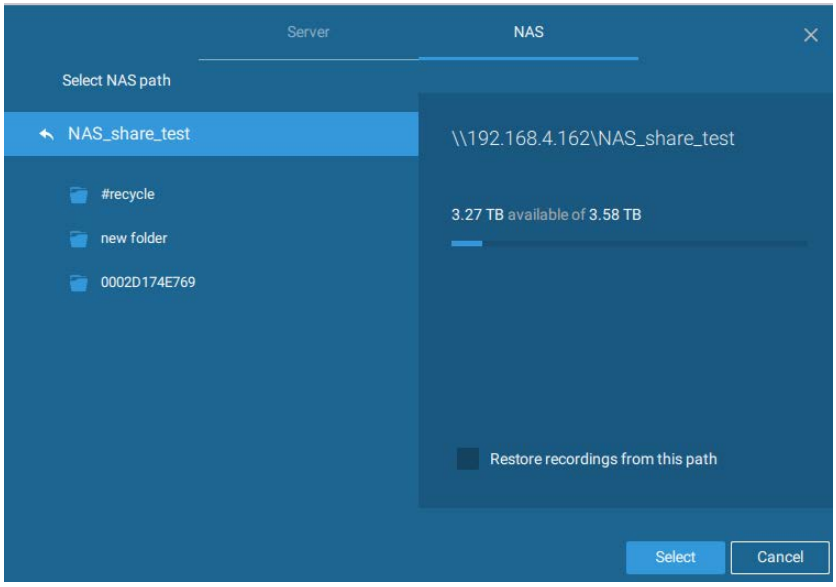
6. The NAS storage should appear on screen. The connection may take several seconds. Single-click on the NAS storage to select its network shares.



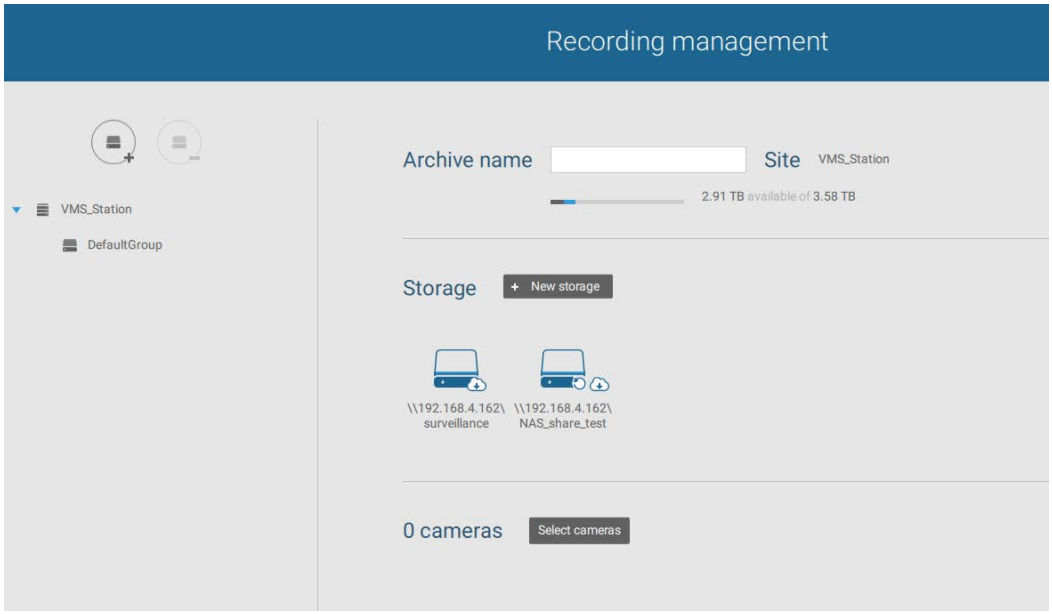
7. The NAS storage's network shares should be listed. Single-click to select a network share.



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



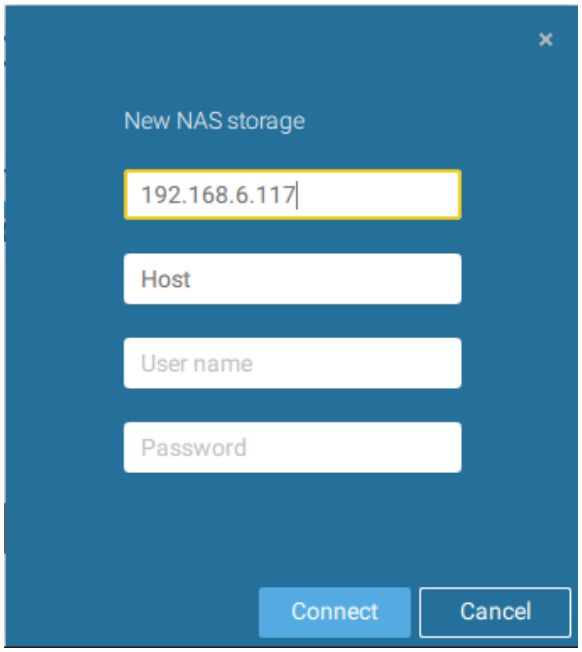
9. The selected shares should be listed. Enter a name and select cameras. When done, click the Add button at the lower right to complete your configuration.

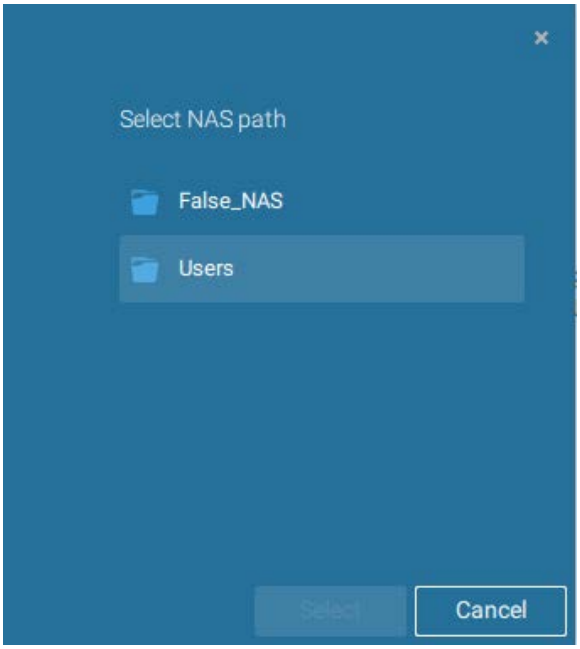


2-2-3. Storage

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.



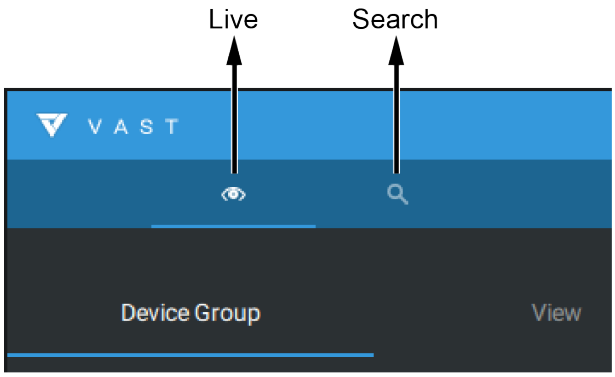


Select storage volumes each by a single click.

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.



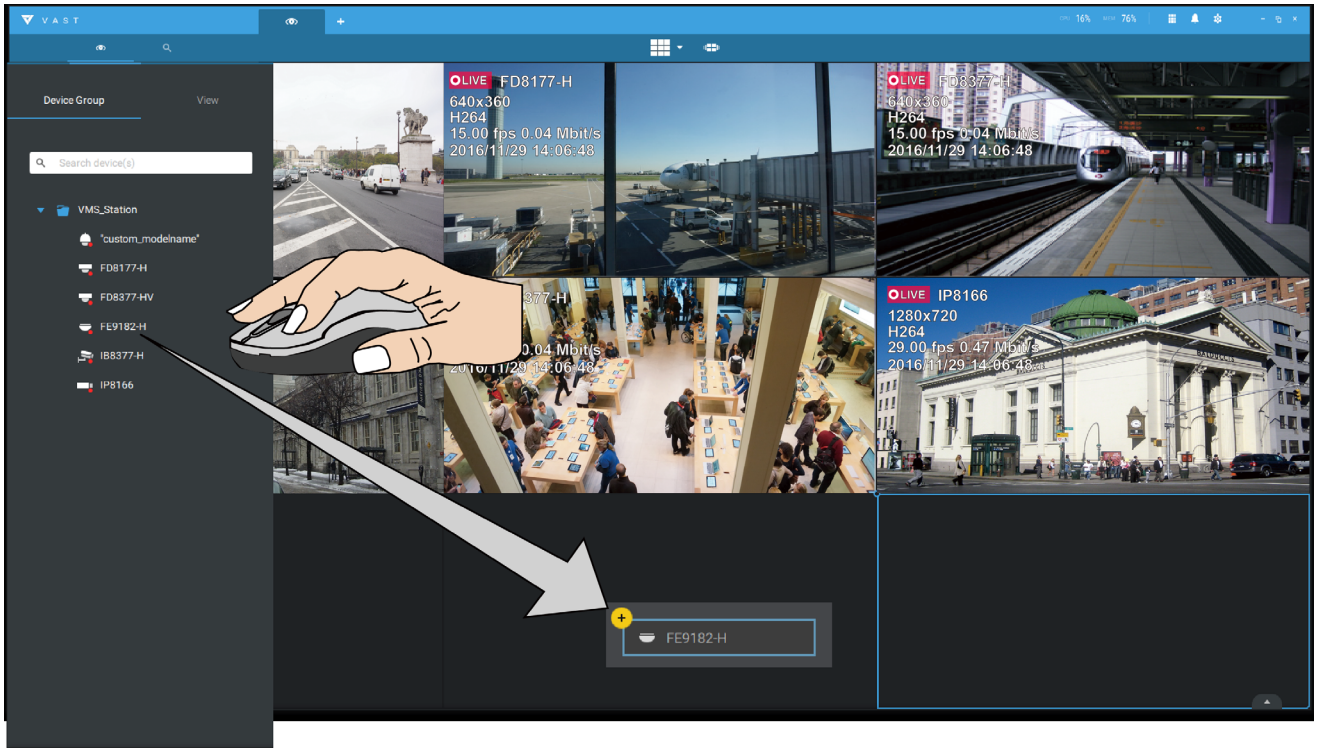
On the initial start up, the server should fill the live camera feed to the available 2x2 view cells (4). You should then select a preferred layout, e.g., 3x3 or others, using the Layout pull-down menu.

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.

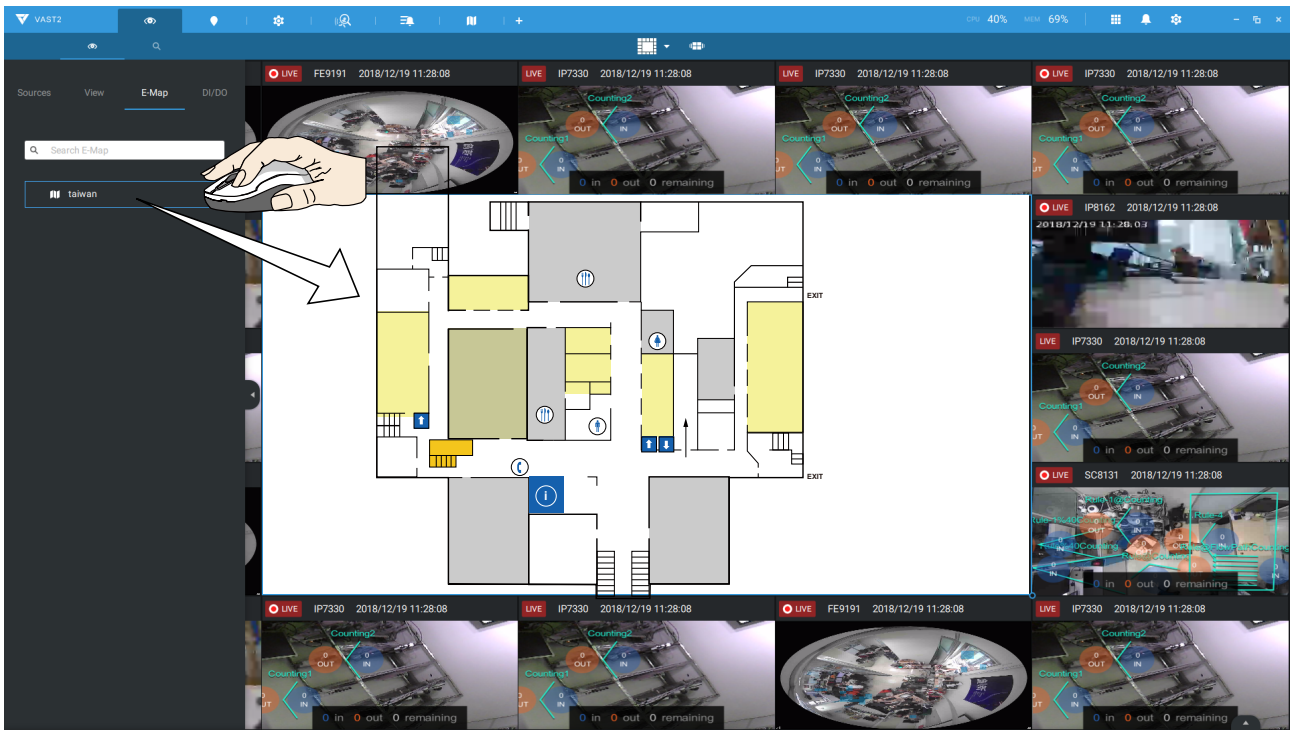
You can then fill in the view cells by dragging and dropping cameras into the view cells. While dragging, a name tag displays. All cameras should be listed under the VMS_Station Device Group.

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.

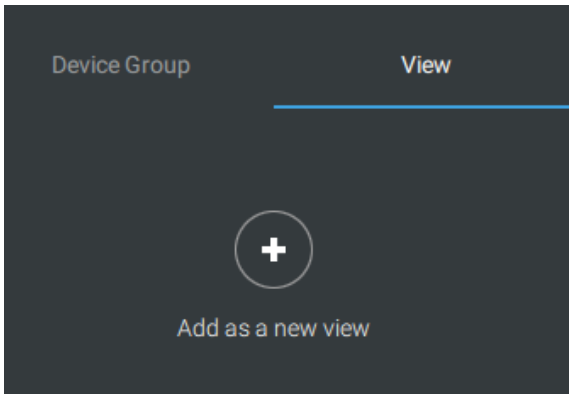
Depending on the resolution of your monitor, a view cell can be too small for an E-Map.
For example, for an HD monitor (1920x1080), a single view cell from a 3x3 layout will have a resolution of 640x360. View cells larger than 330 (width) x 300 (height) pixels can contain an E-Map.

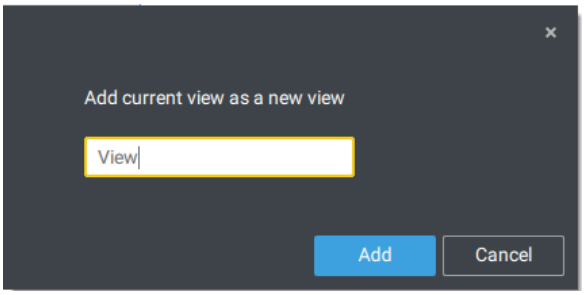


2-2-5. Saving a View

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

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

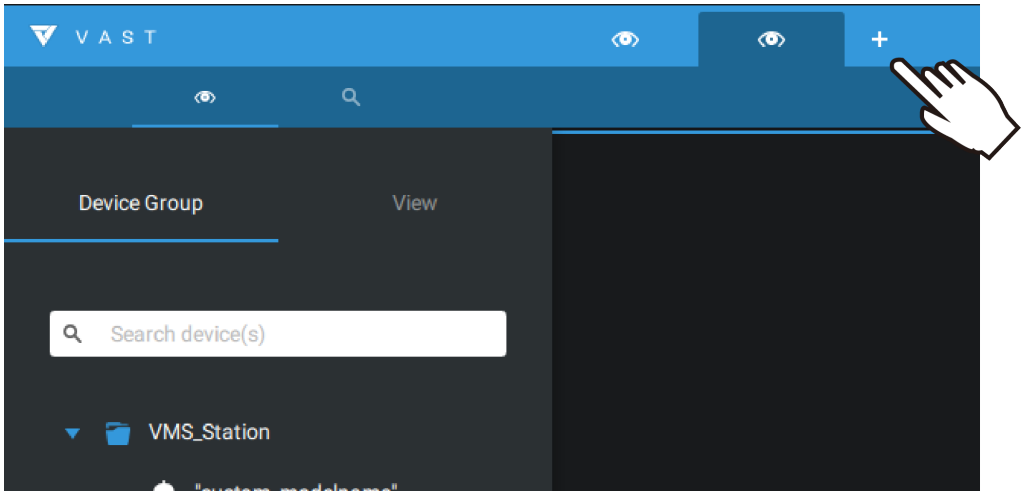




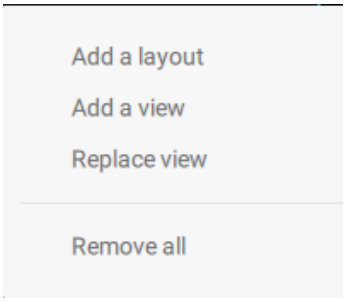
2-2-6. Add More Live Views

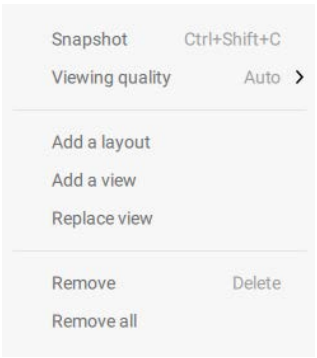
With many cameras in your deployments, you can click the New Tab "+" button to add more Live views.

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.

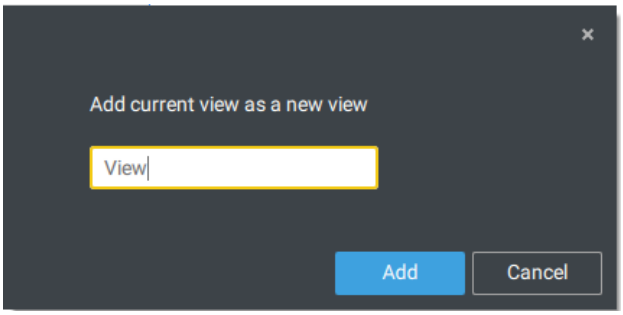


Right-click on the screen to display the right-click menu. Select **Add a view**.



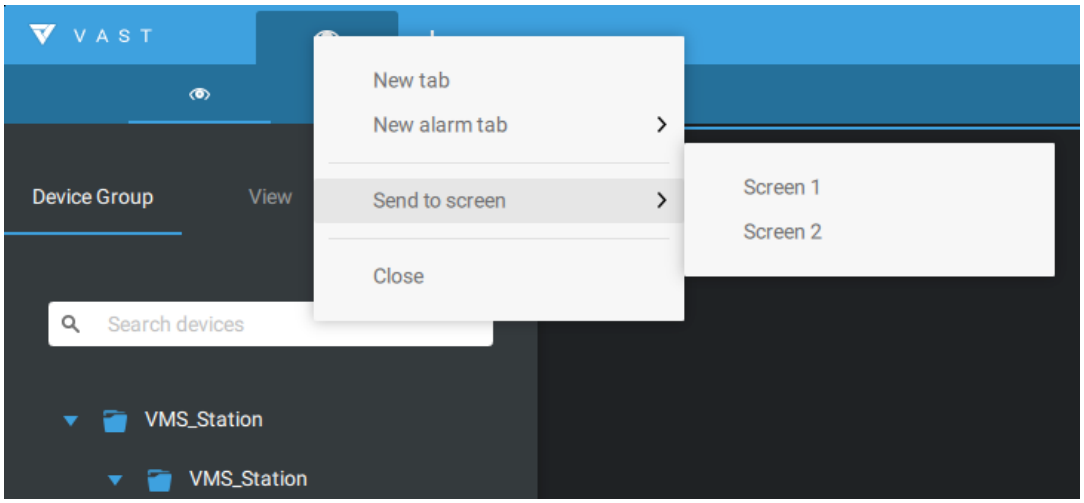


Enter a name for the new view and click **Add** to proceed. The new view will be listed in the View panel.



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.

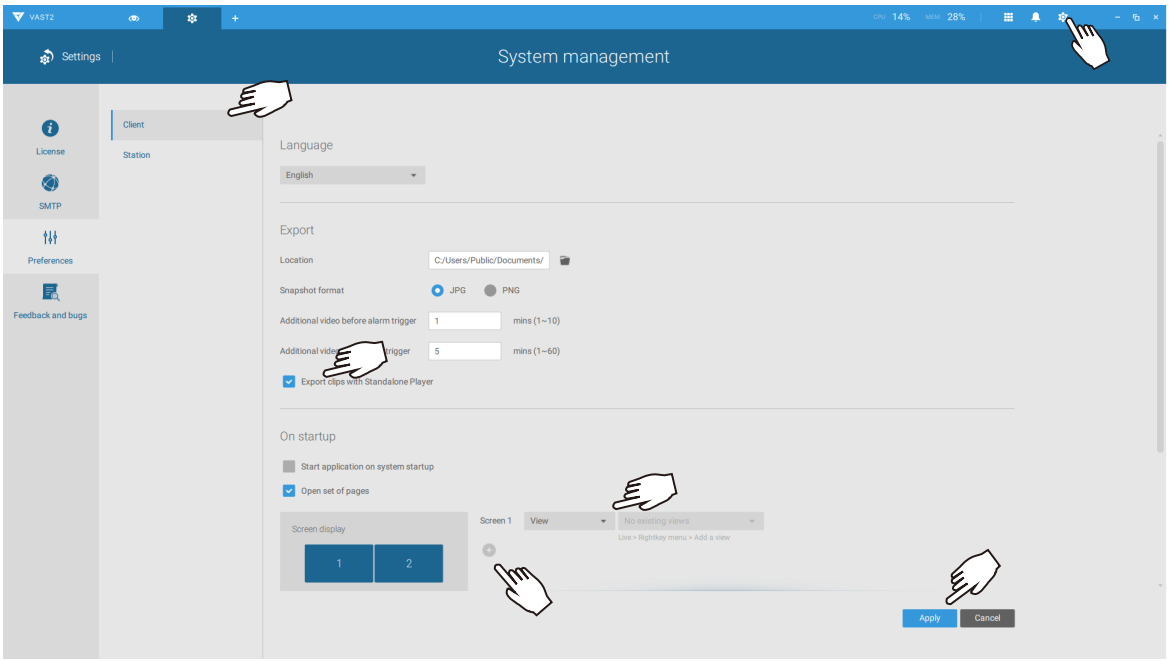
Live views can be placed on up to 8 monitors. Please note that this is determined by the capability of your graphics card chipset.



2-2-7. Save Your Preferences

Go to **Settings** > **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.

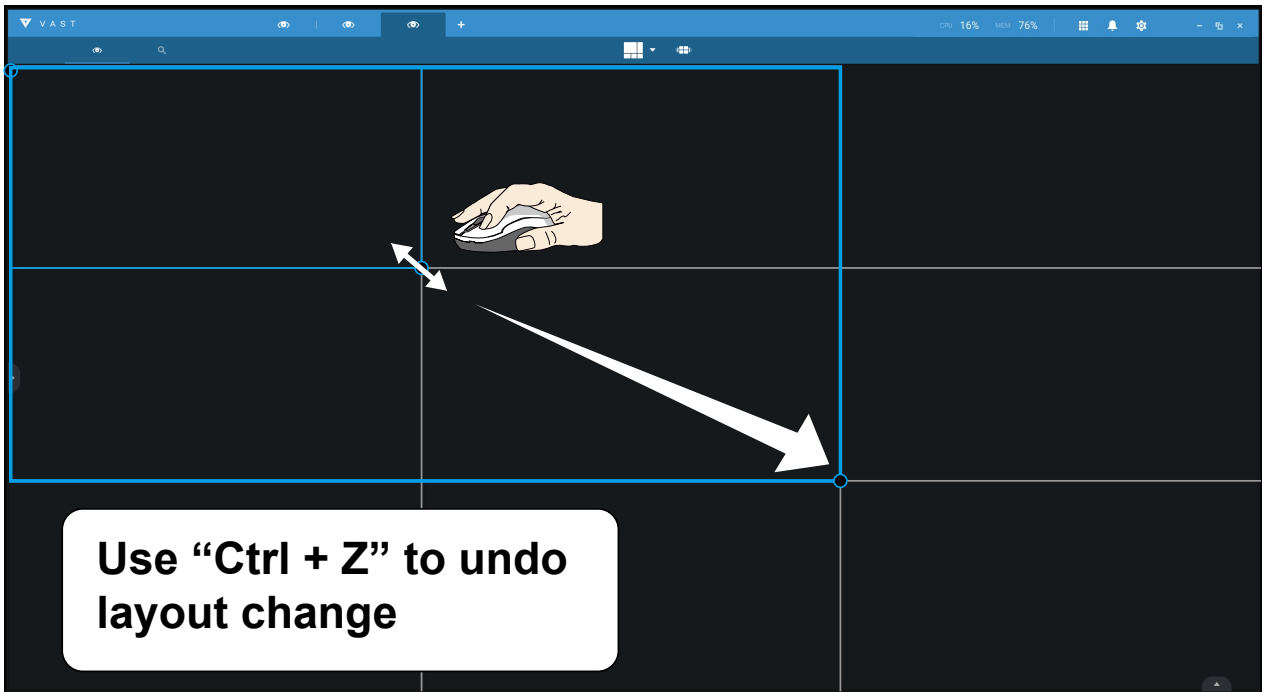


2-2-8. Customizable Layout

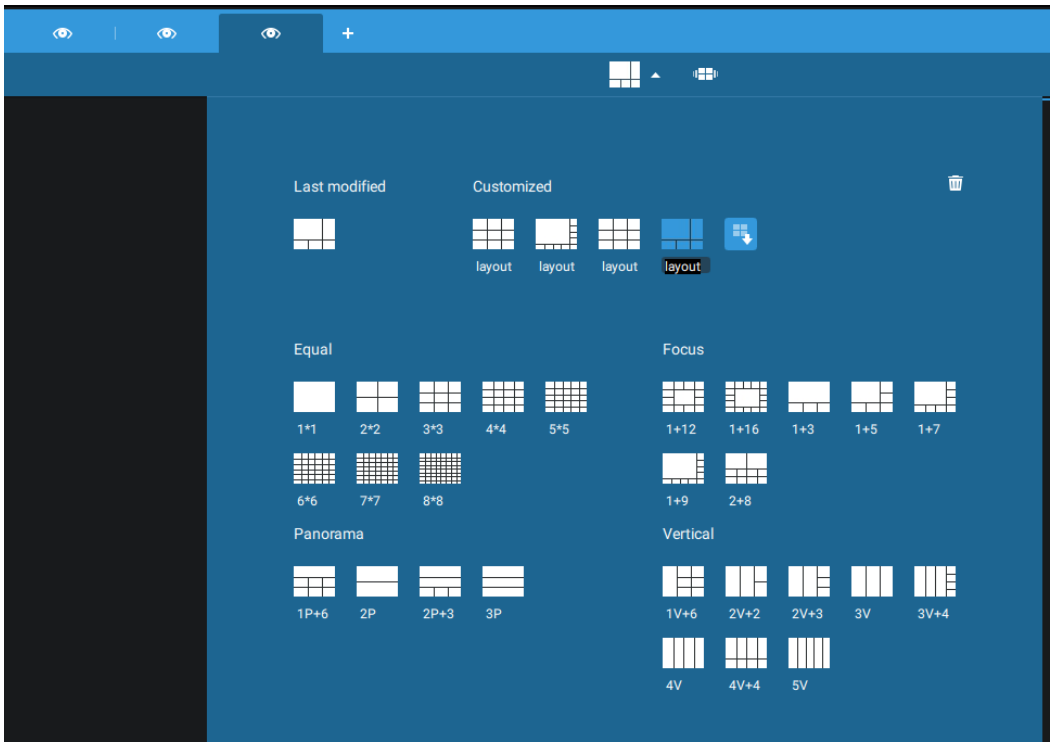
The standard layouts can be manually configured to form layouts of your choice. Depending on the complexity of your design, you should start with a multi-cell layout.

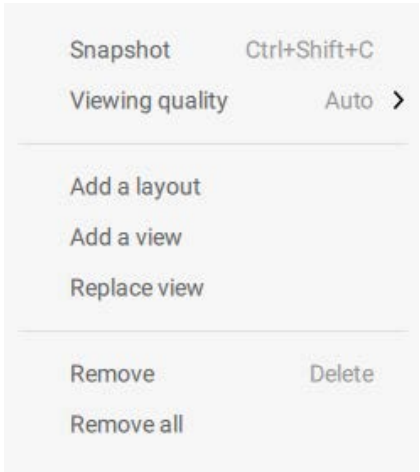
Click and drag the corner mark on a view cell. Drag across the screen and release the mouse button to enlarge the view cell. Choose a standard layout of many view cells, e.g., 7x7 or 8x8, if you want to design a complex customized layout. You can create a special layout, e.g., an especially wide view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





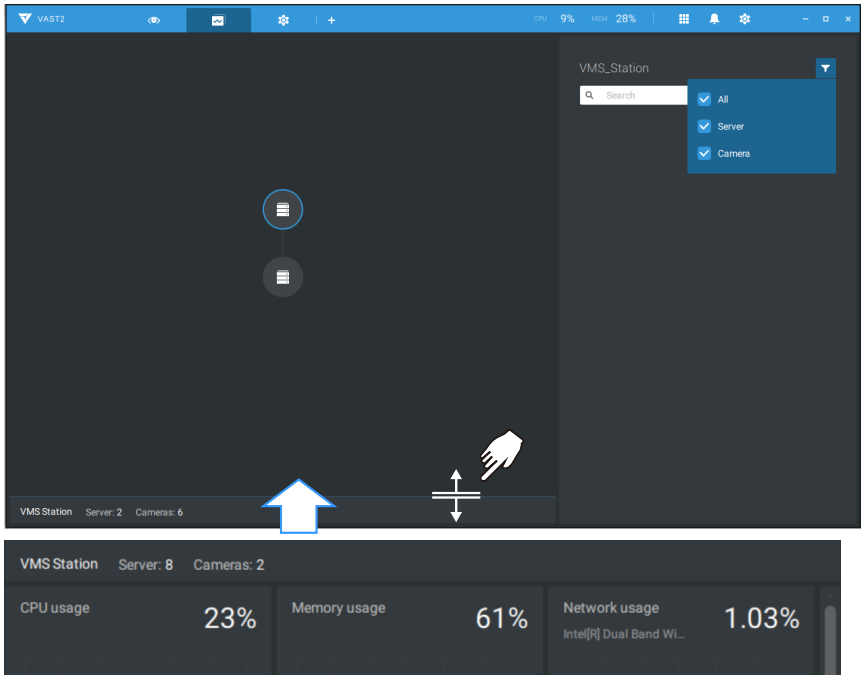
You can also right-click on the screen to display the **Add layout** option.
You can then click Device Group, and start filling your customized layout with camera views. When done, click **Add a view**.

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

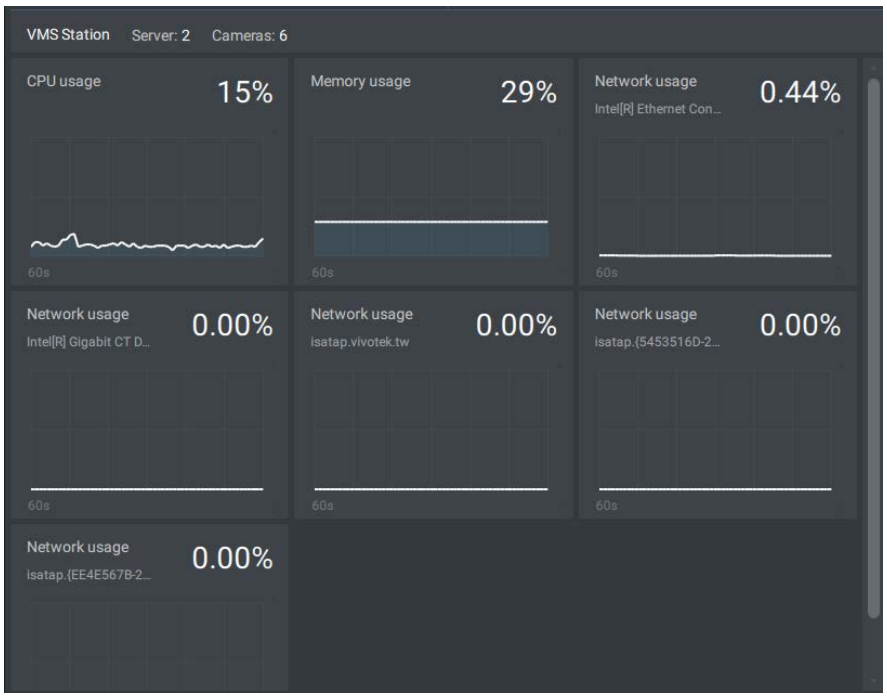
2-2-9. Dashboard

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.

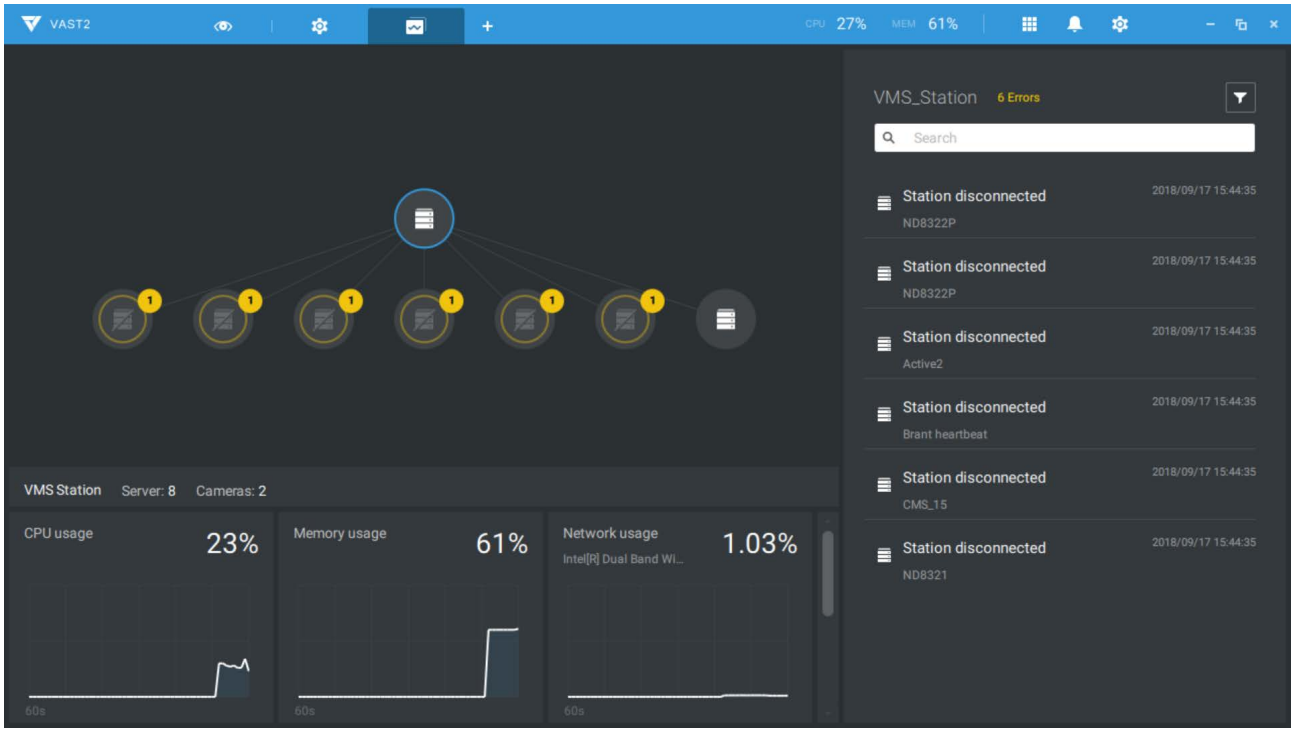
Mouse over the edge of the bottom row to reveal the expansion mark. Pull the status row up to display the system resource statuses.



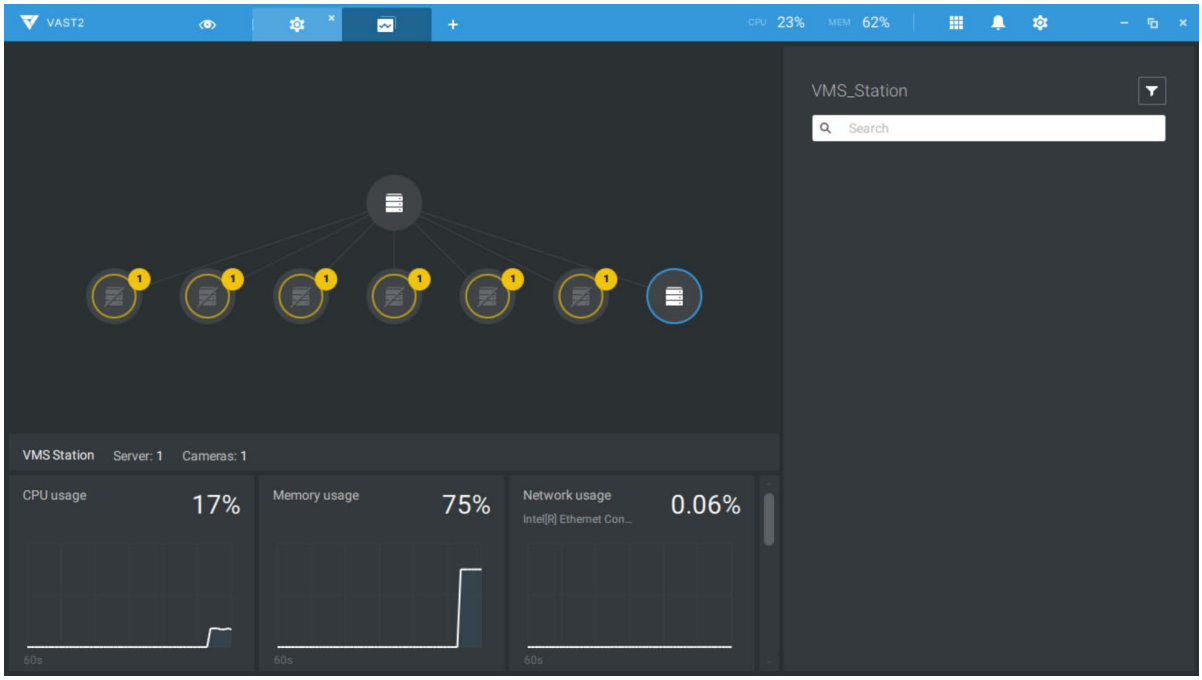
If you have multiple LAN cards or virtual HBAs, the status row can be pulled to reveal all of their statuses.



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.



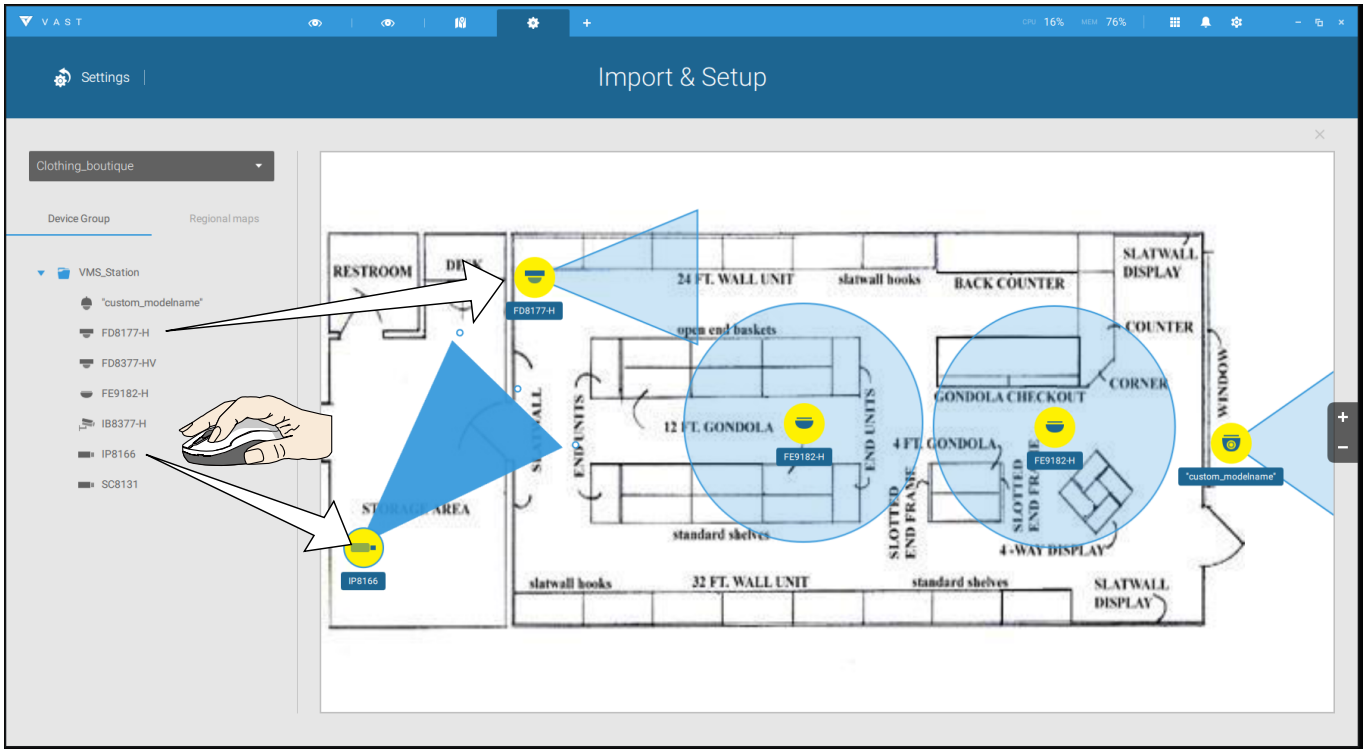
2-2-10. E-Map

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

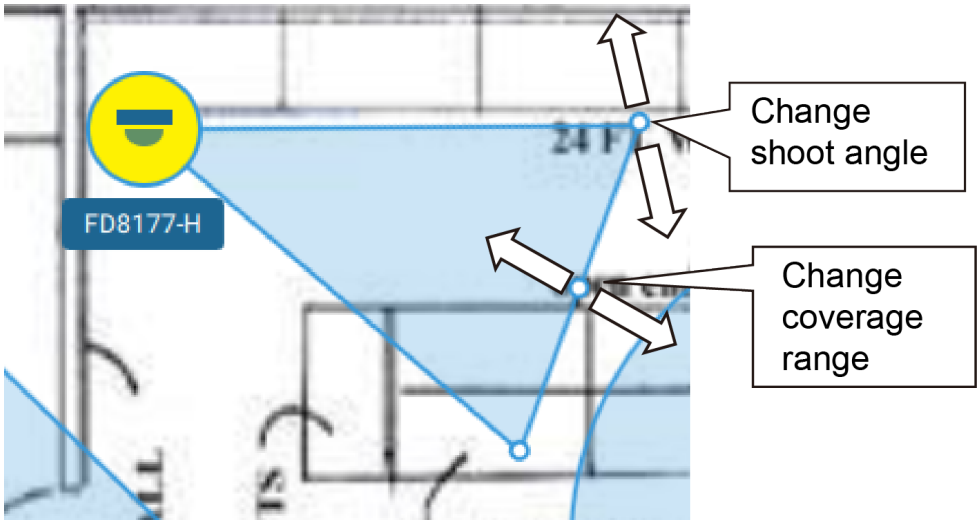
Click Import file or Import folder . An entire folder can be imported.

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

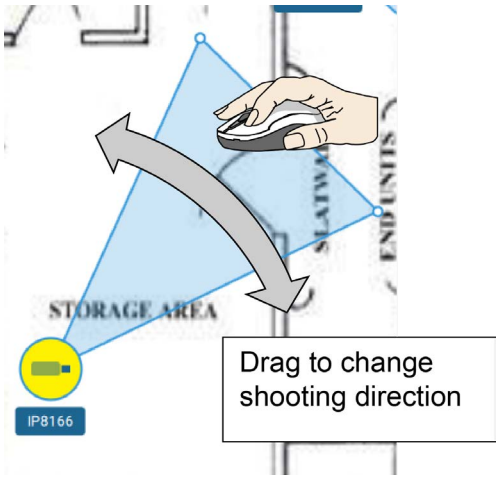
Your cameras will be listed on the left. Drag and drop the cameras to the corresponding locations on the map.



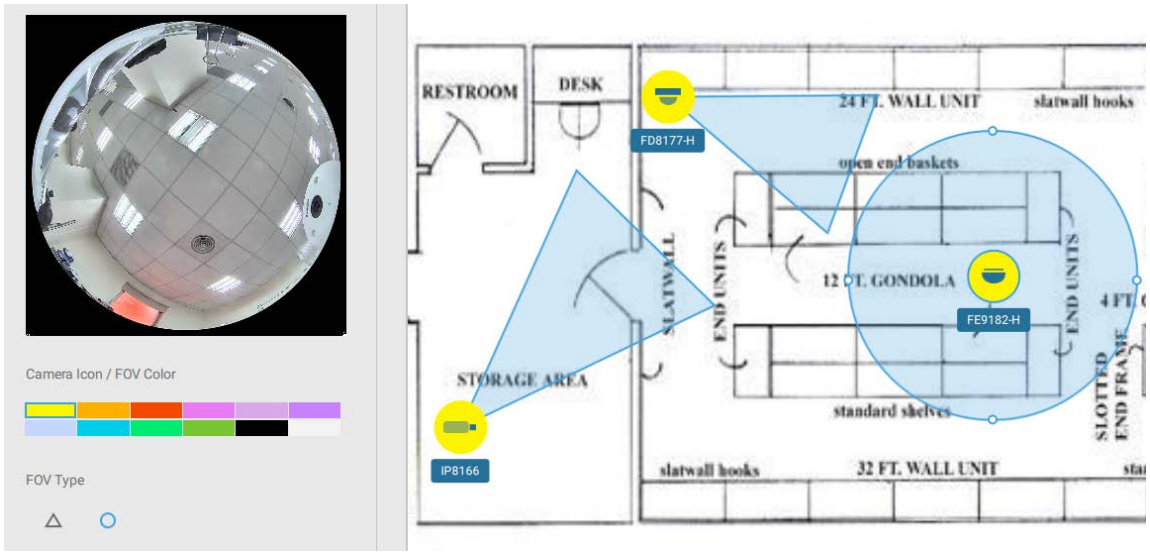
When the camera is in place, drag the FOV indicators on the edge to change the shooting angle and the coverage range.



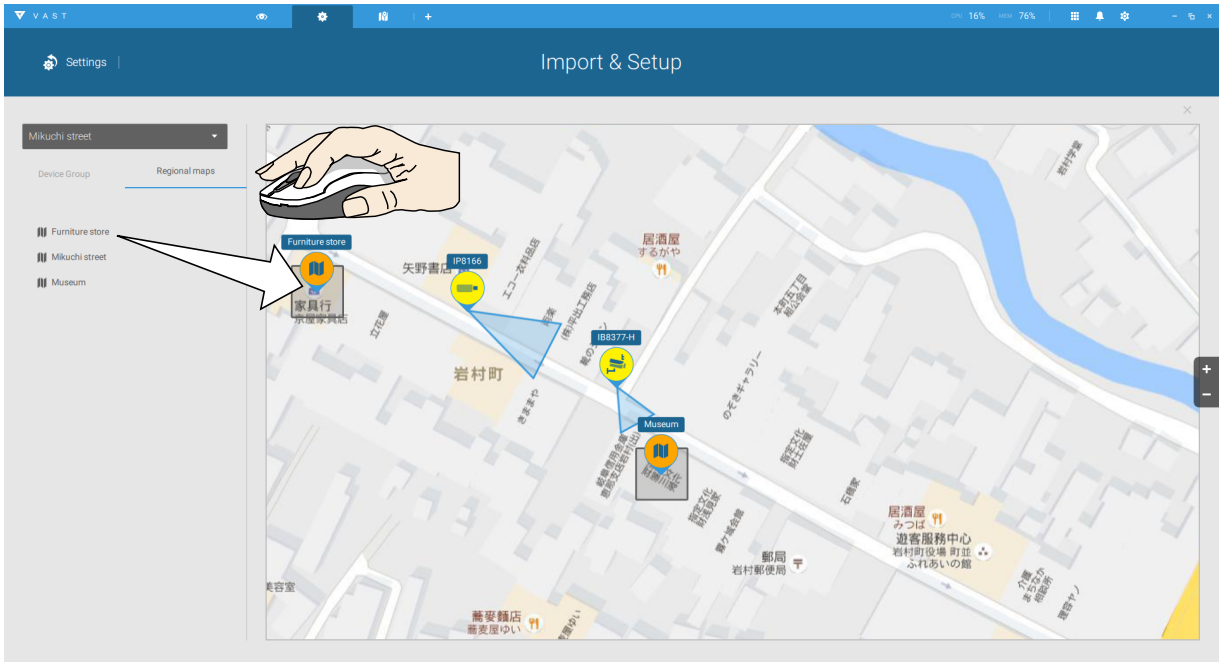
Drag the FOV to change the shooting direction to match the actual installation.



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.

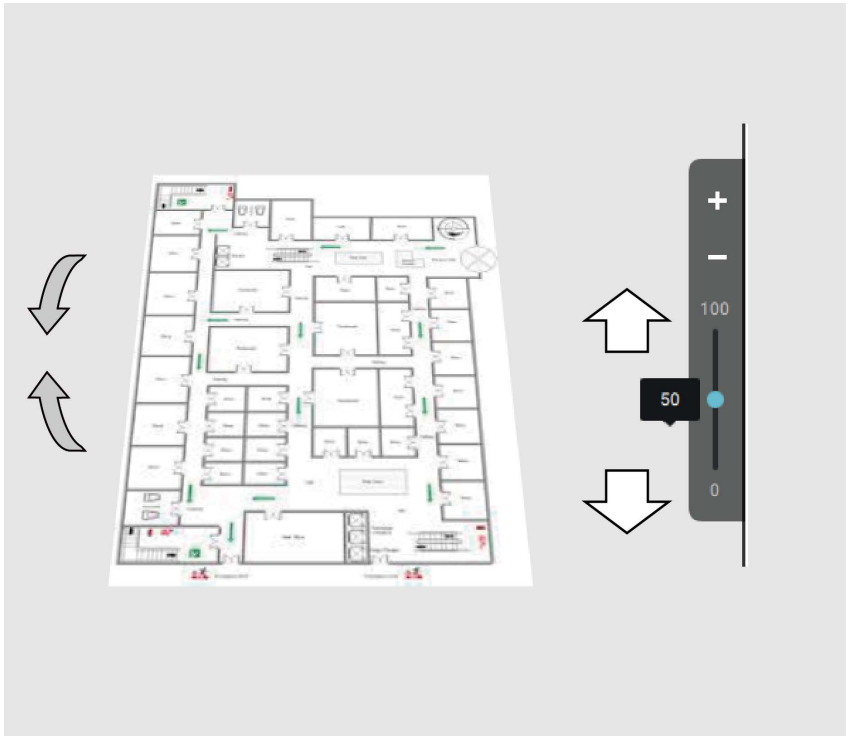


If you have a larger regional map that covers a geographical area, say, a street block, you can drag one or many E-Maps into it. For example, you can place another E-Map that is used to indicate the camera deployment inside a building that is located on the street.



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.



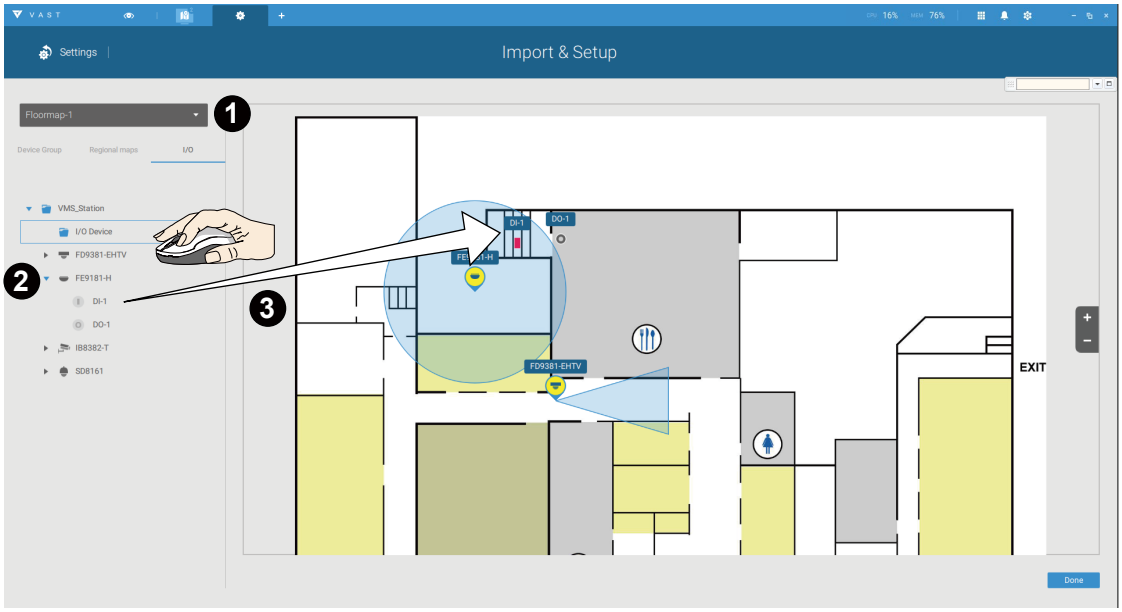
Placing DI/DO Devices

I/O devices can also be planted into an Emap, such as alarm or various kinds of detectors. The I/O boxes (such as Advantech's Adam series) or the DI/DO connections on an NVR also apply.

1. Select a floor map from the pull-down menu.

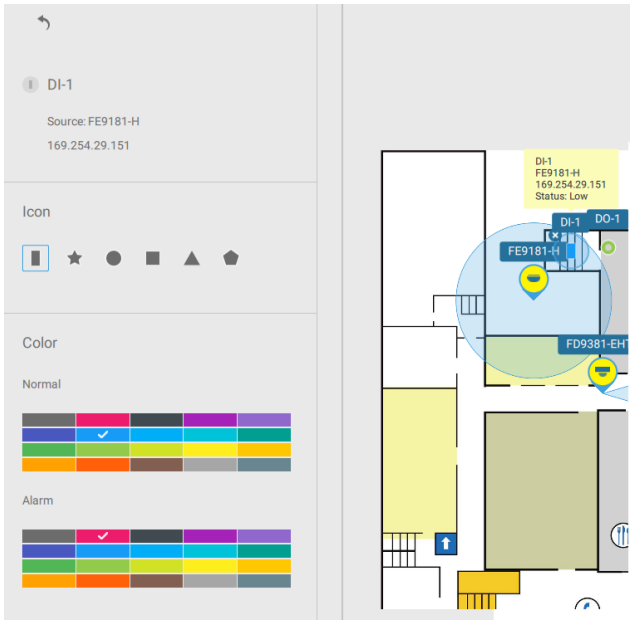
2. Unfold the sub-trees beneath the network camera, (taking camera DI/DO devices as an example).

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.

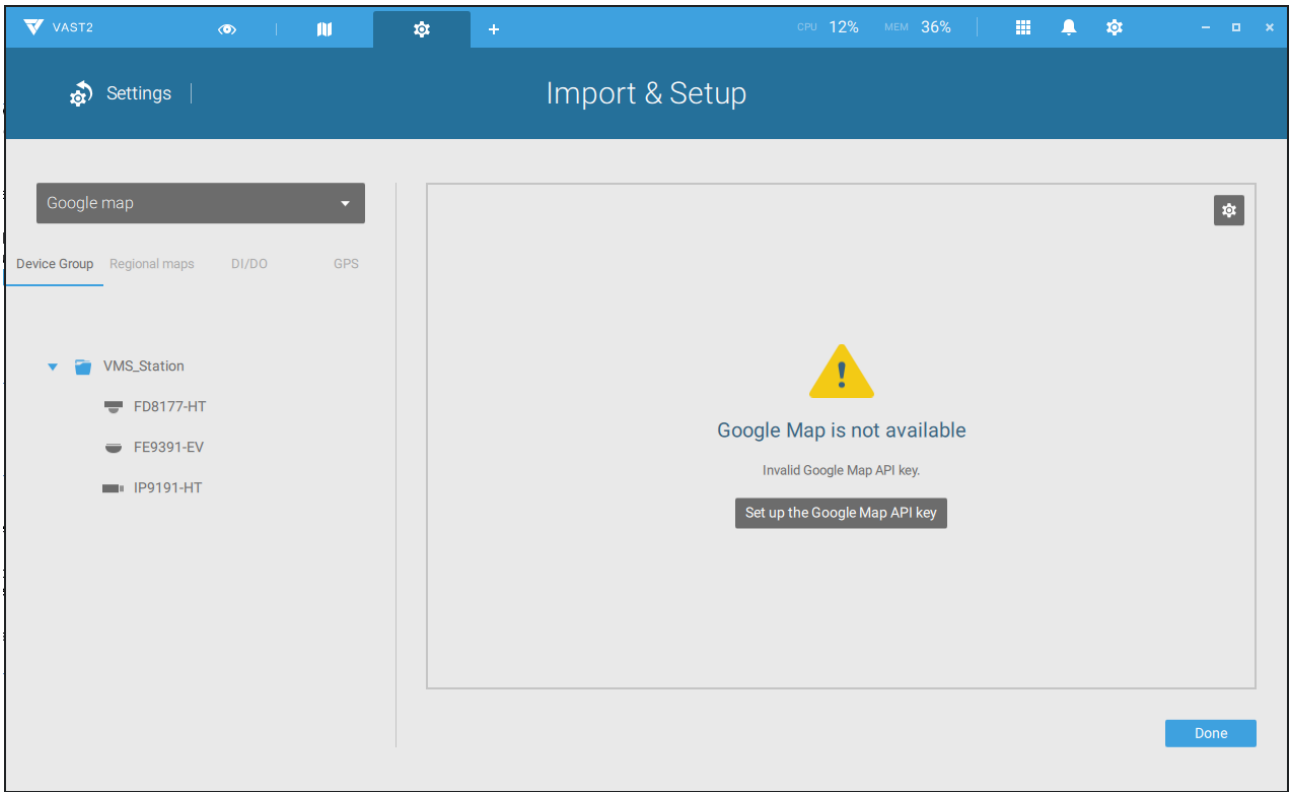


Configuring Google Map and GPS

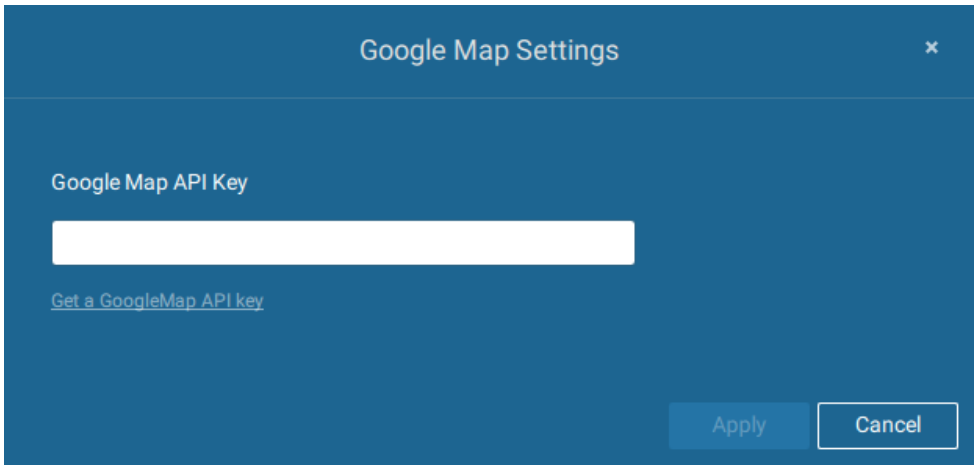
Since Google Map changed its access policy, using the Google Maps feature requires user entering a billing API key. Using Maps, Routes, and Places APIs requires an API key.

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

Visit Settings > Emap > Google Map.



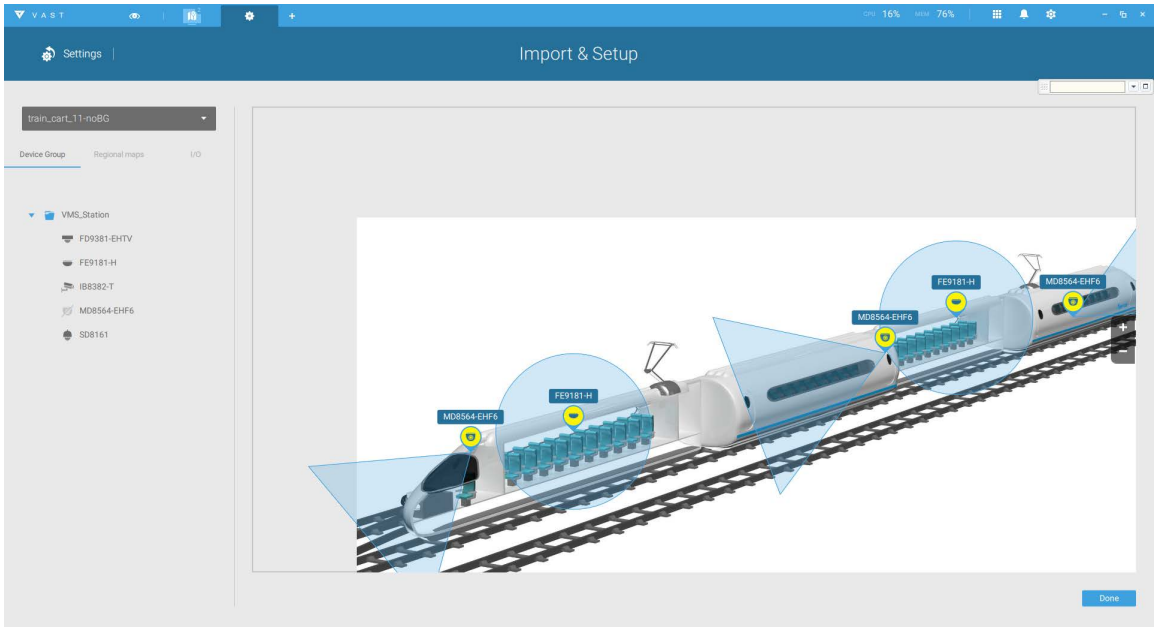
Enter the Google API key you previously registered.



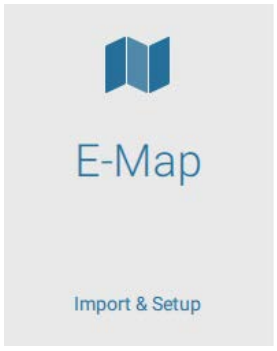
NOTE: In this revision, Google Map only supports installation on a GPS-enabled vehicles. Placing cameras on a static location on Google Map is currently not supported.

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.

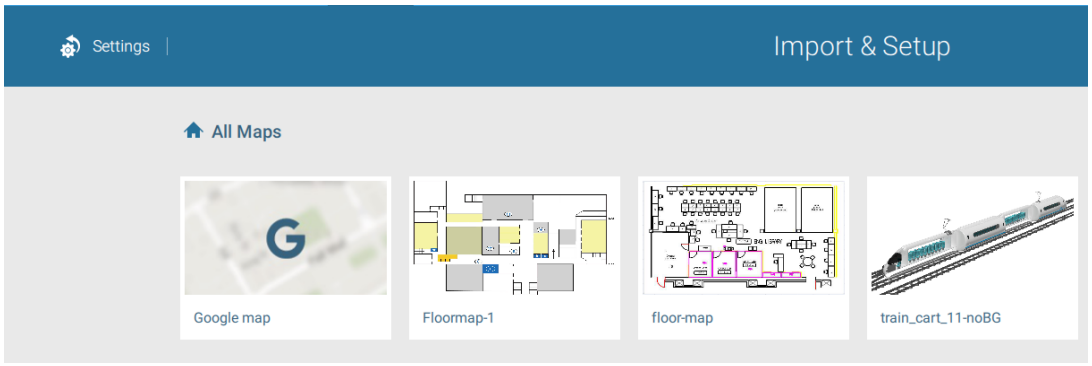
This applies to a mobile NVR that comes with GPS.



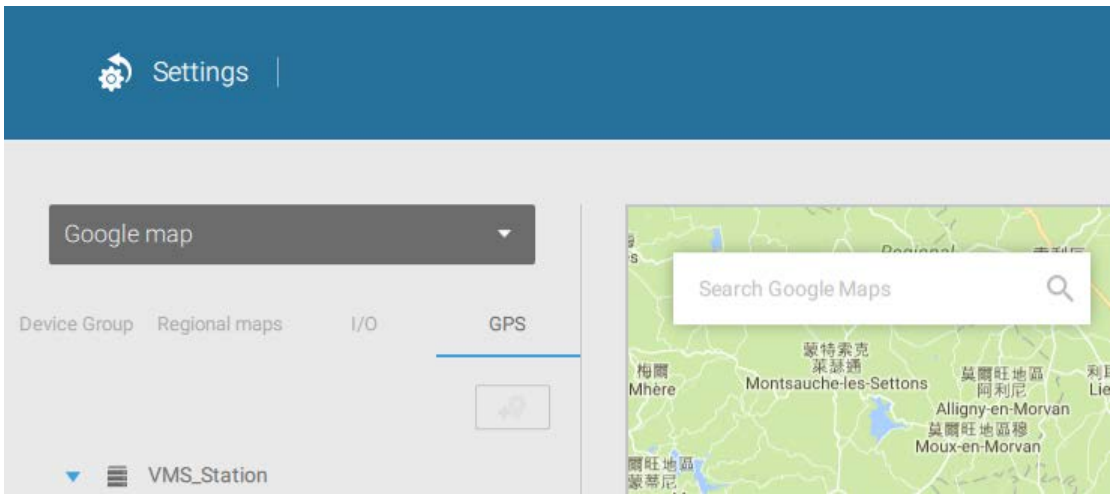
Open the E-Map Import & Setup window.



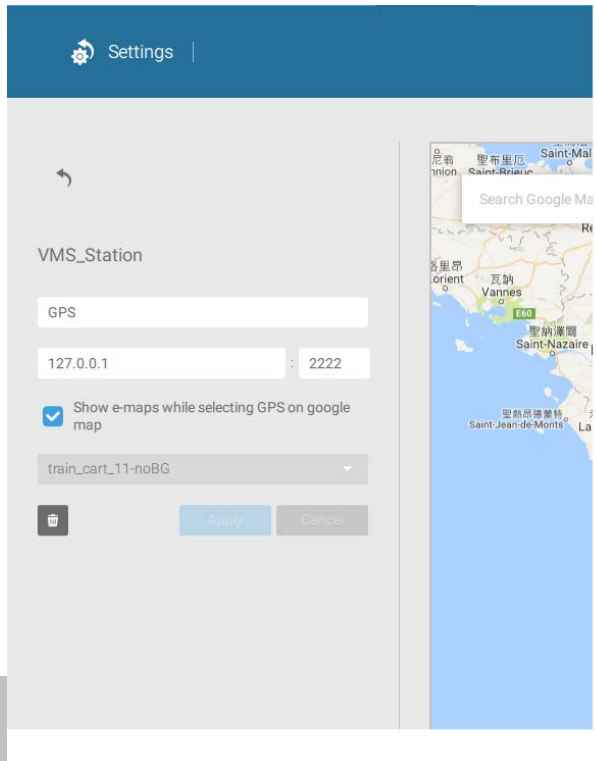
Click to enter the Google Map window.



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

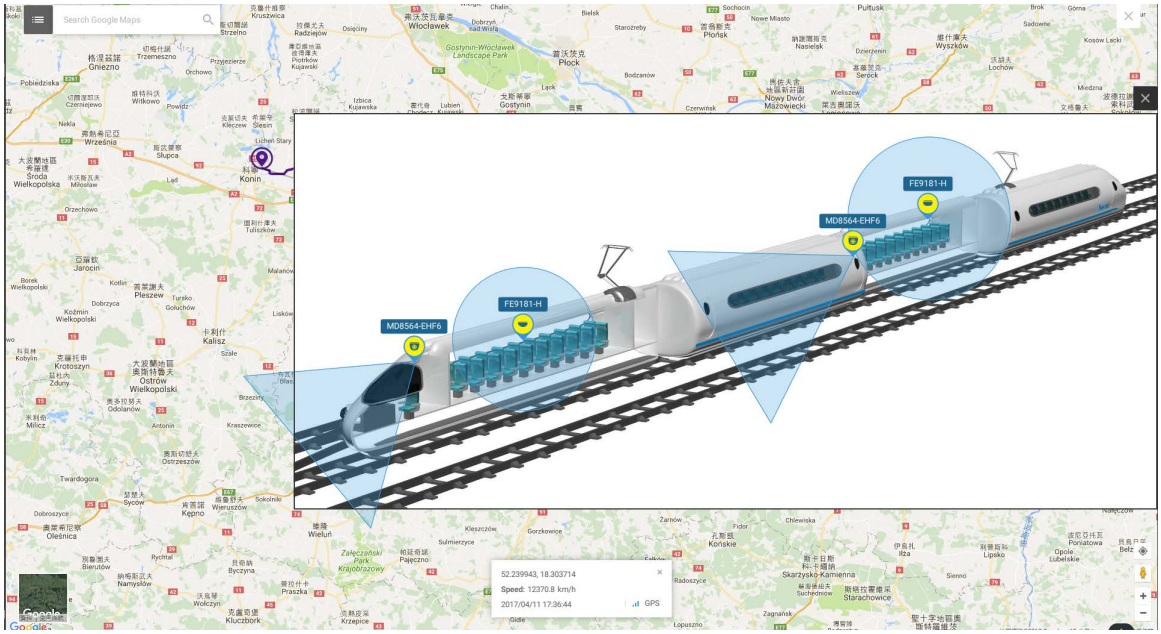


Enter a name for the GPS/GNSS server on the vehicle, its IP address, and server port number. You can select an E-map that will display when you click on the GPS location icon. Select the checkbox and an E-Map that corresponds to the deployment on the vehicle. When done, click the Apply button.



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.

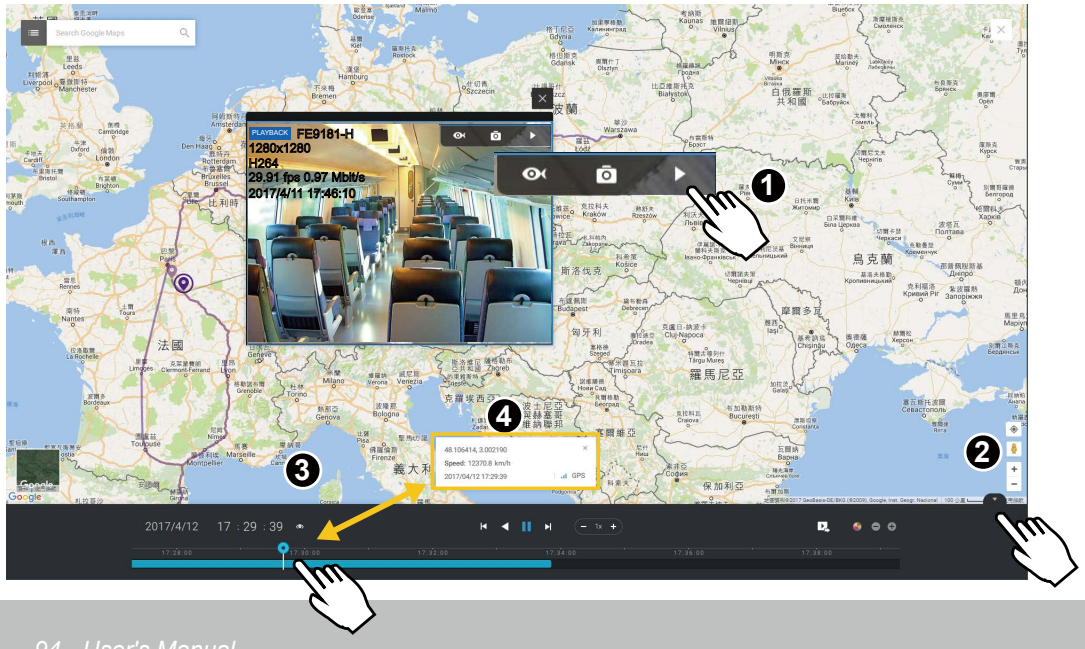
To search and review recordings when an event occurs,

1. Click on the Playback button.

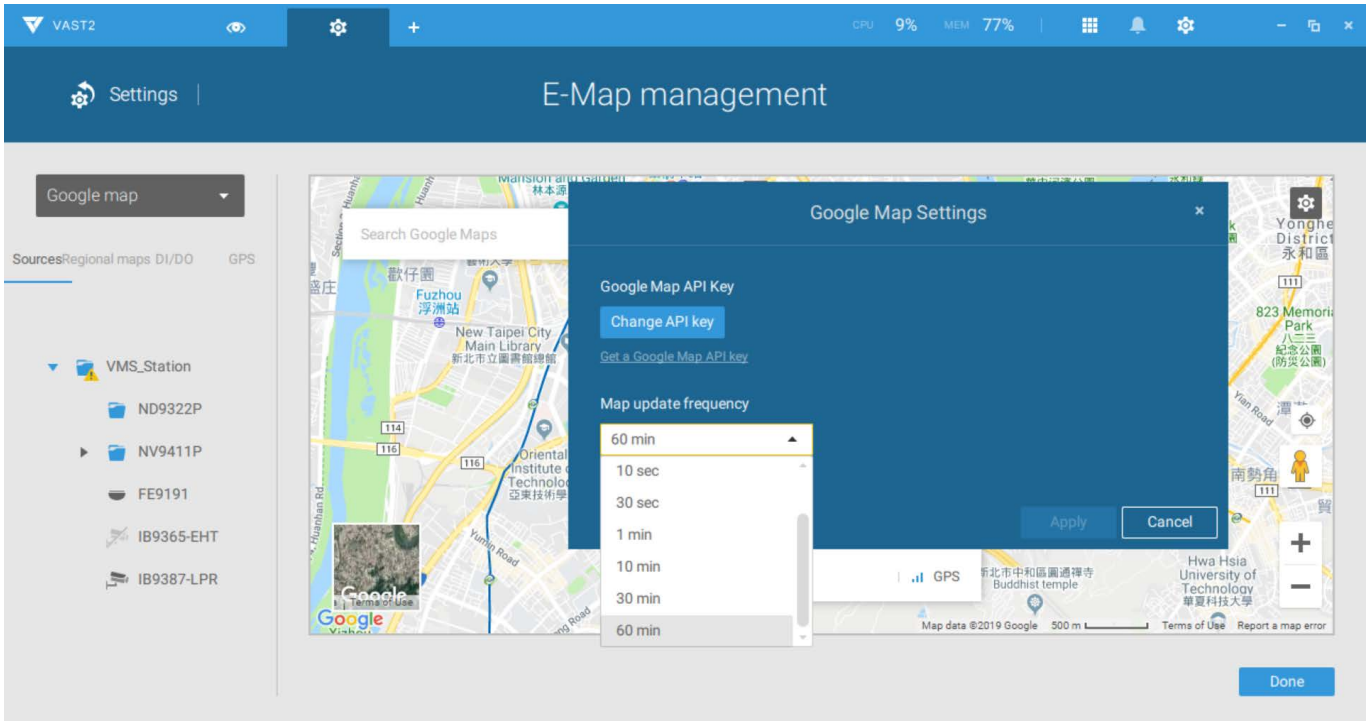
2. Click the Pane button to display the Playback control panel.

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.

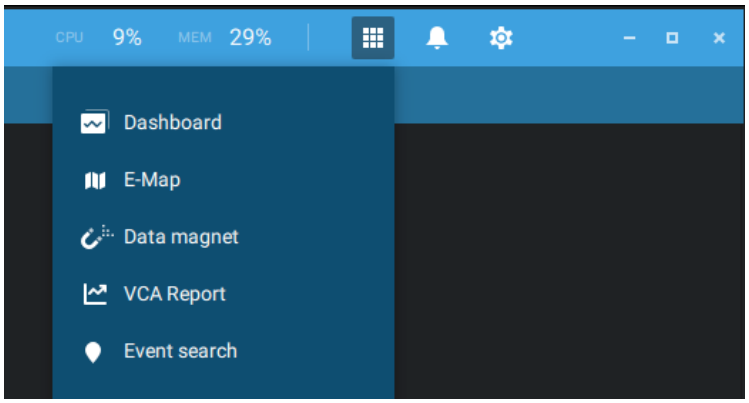


Click on the Setting button on the map to bring up the Map update frequency option. Your GPS target may travel to the outside of the map through time without the map being updated. The map will update by the interval you configure here.



2-2-11. Event Search

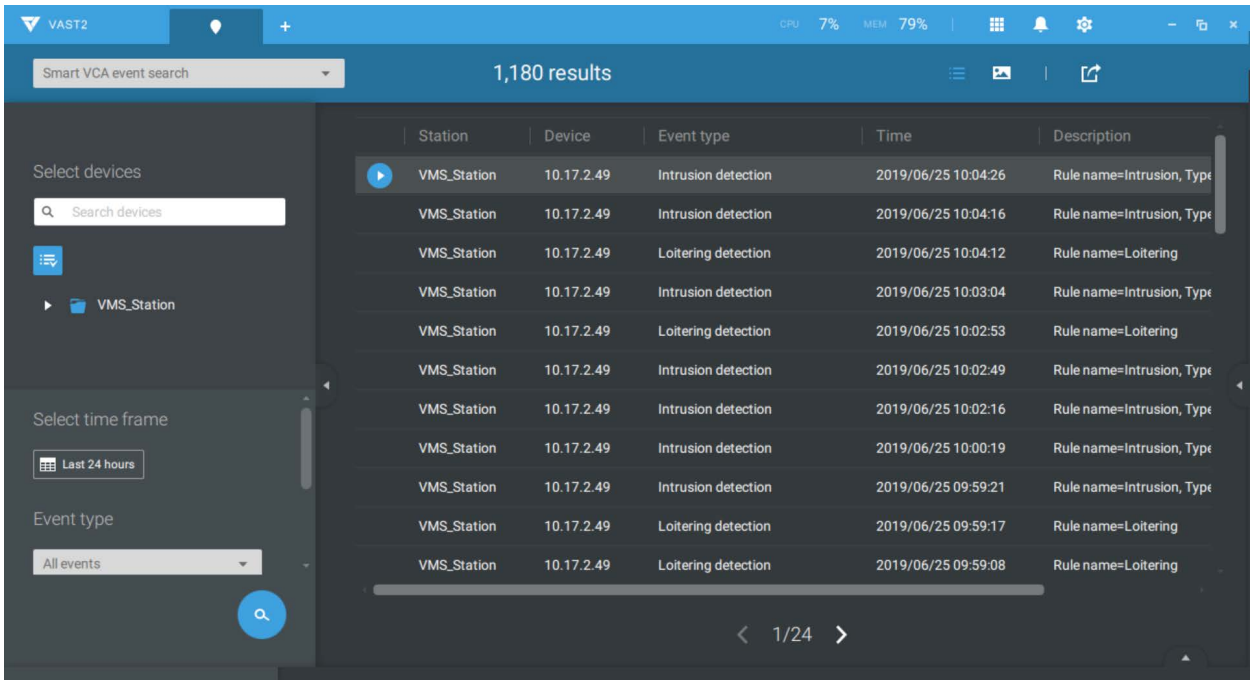
The Event Search window is accessed from the top tool bar.



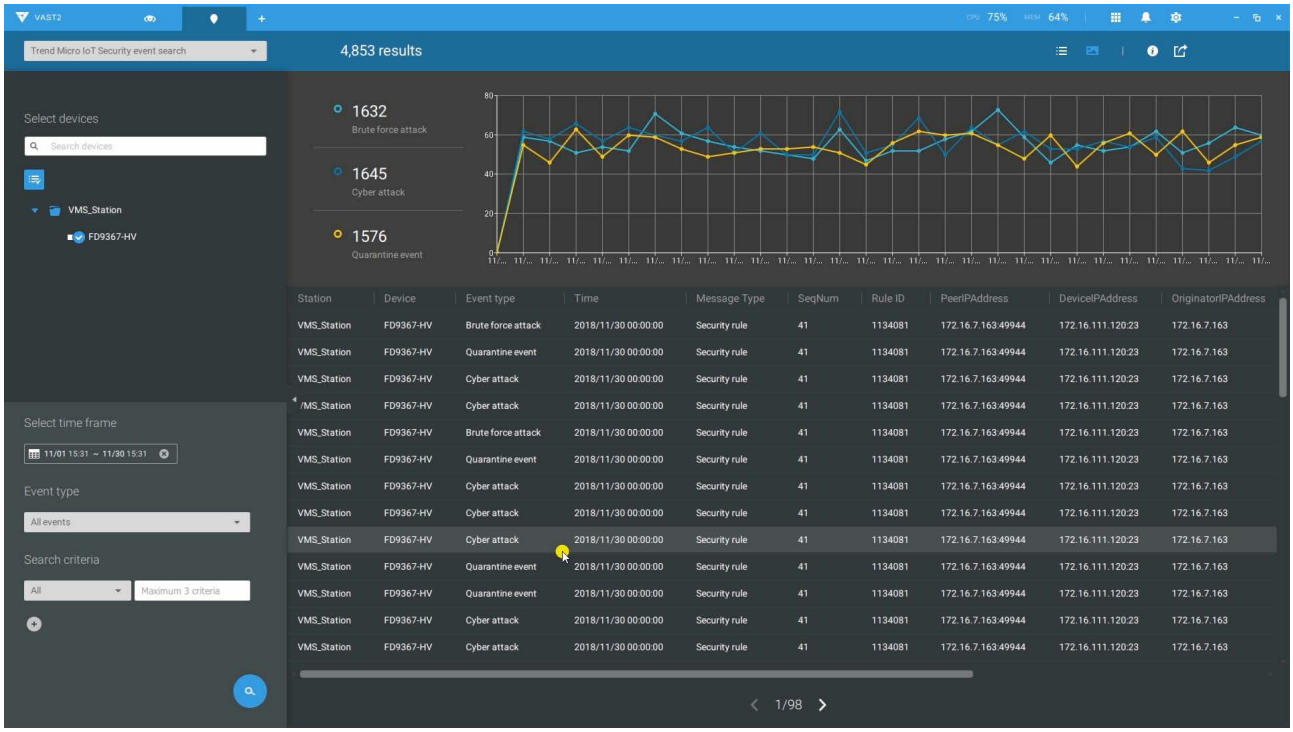
Below is the comparison between the Alarm list and the Event search windows:

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.

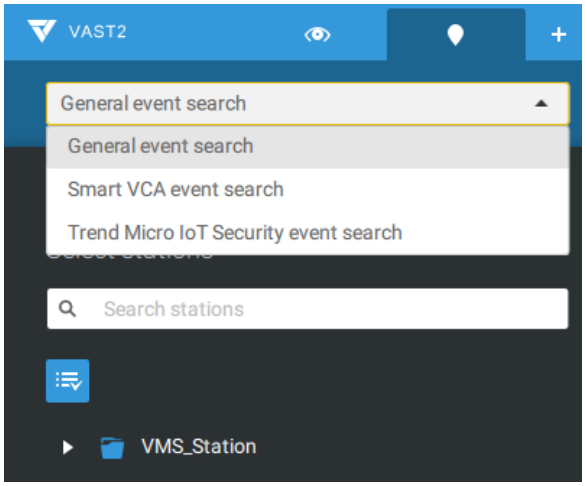
The sample screen for VCA-related events is shown below:



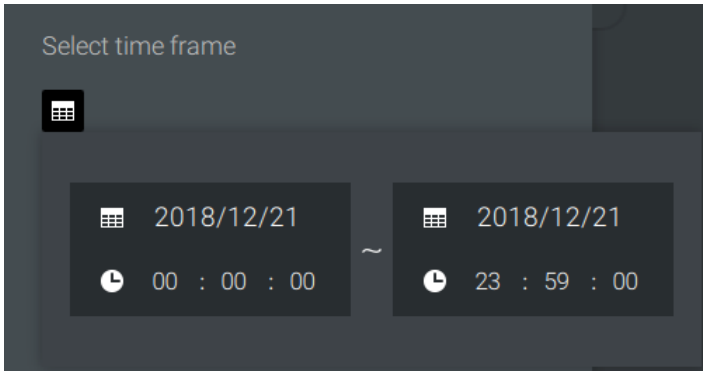
The sample screen for network security-related events is shown below:



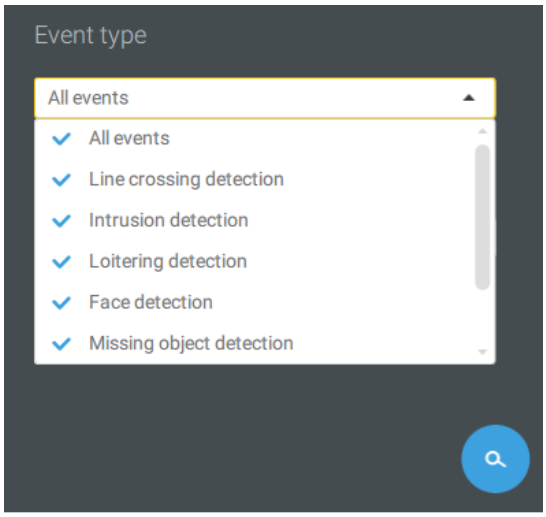
From the Search Event window, you can view and search events by its event types, and use the Export button to save a record of these events (in the CSV format).



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.

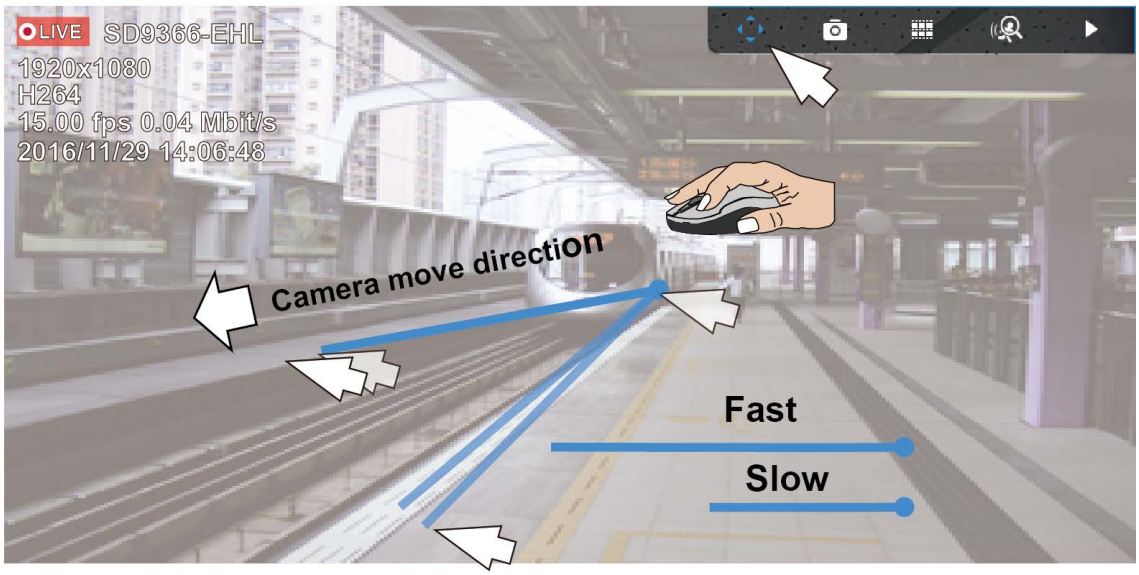


Click the search button to generate search results.

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.



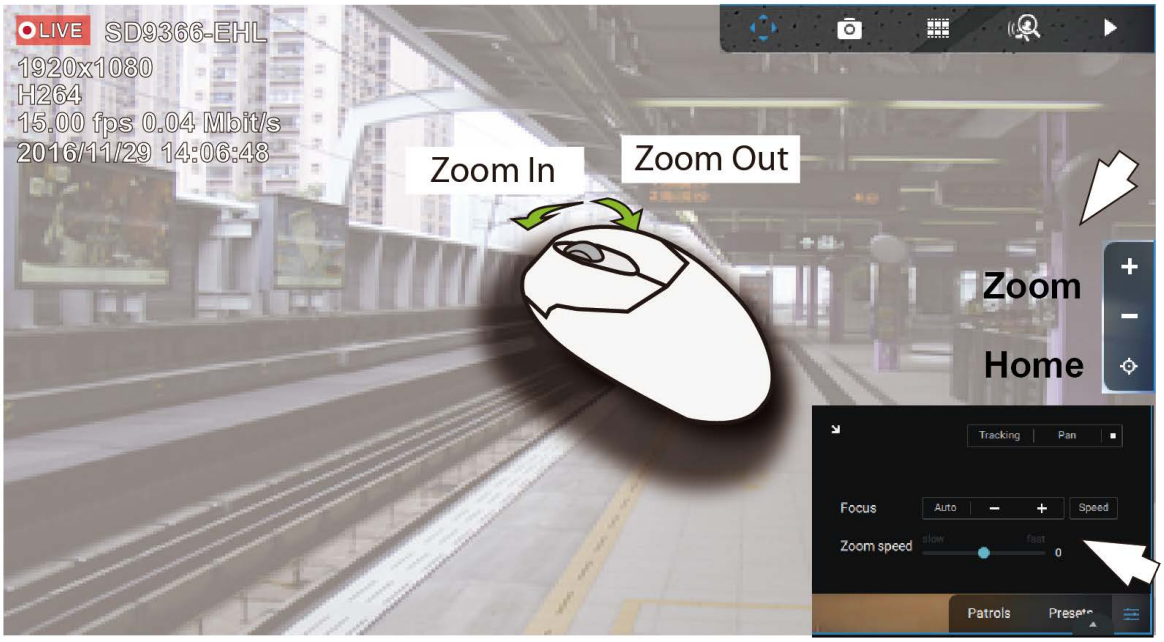
Note that while the camera is moving, you can change the move direction keeping the mouse button hold down. Release the button to stop moving.

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 an Auto tracking, or Pan action.

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



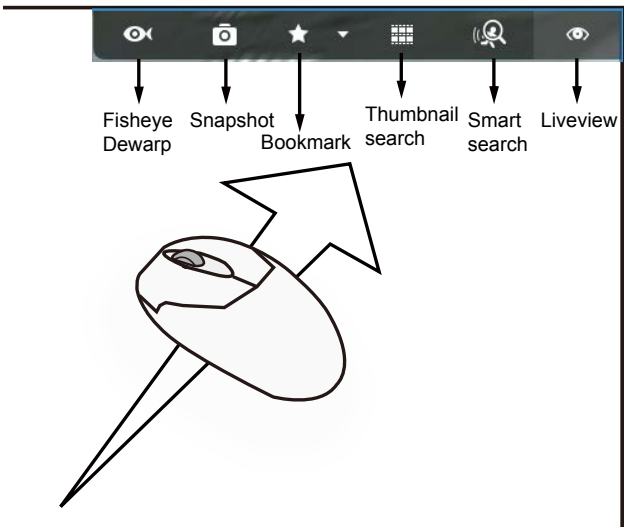
2-2-13. Playback

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 (or). 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:

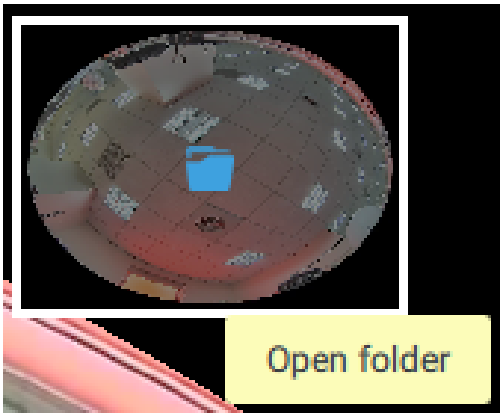
1. **Float Panel**: When Playback is started, swipe your mouse to the upper-right of the view cell to display the Playback float panel.



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.

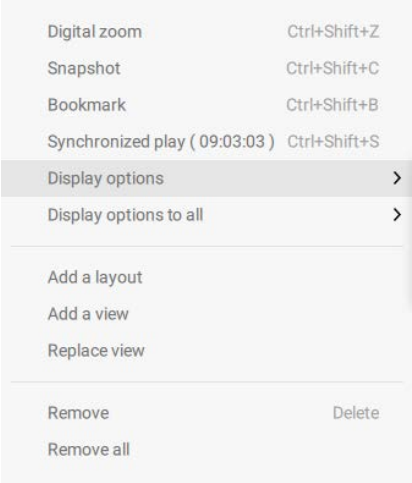


Bookmark: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos. Note that the bookmarked video clips are free from storage recycles. They will not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

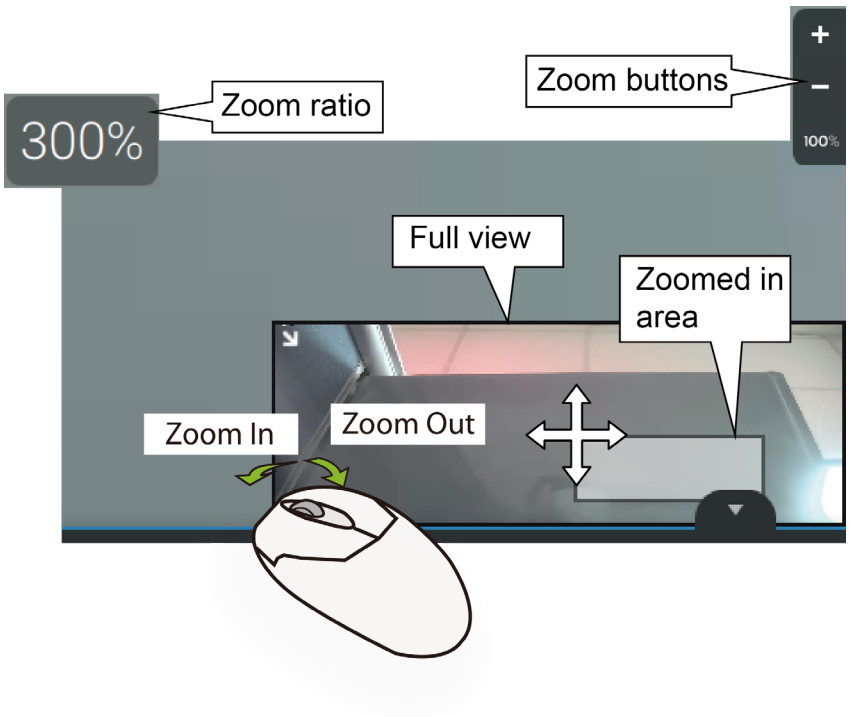
Smart search II: Smart search II is an independent function. See page 122 for details.

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.

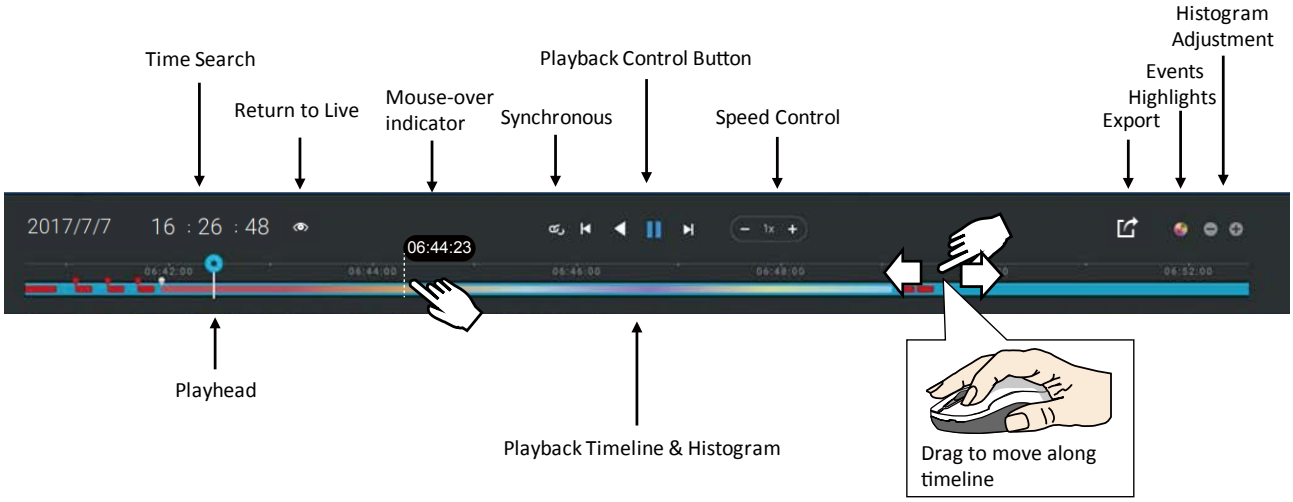
Bookmark: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos.

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.

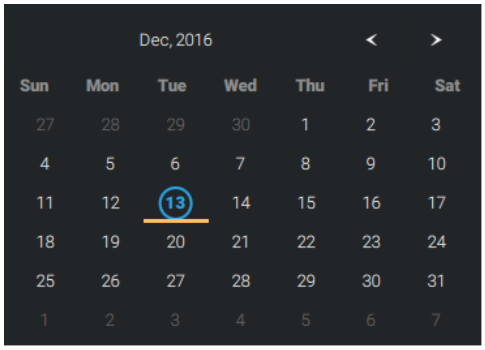
3. Timeline Panel: This panel appears when Playback is initiated.

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.



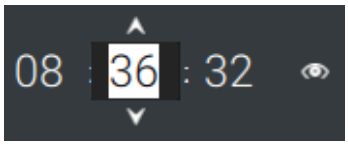
Starting from left to right, timeline control functions will be described as follolws:

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.

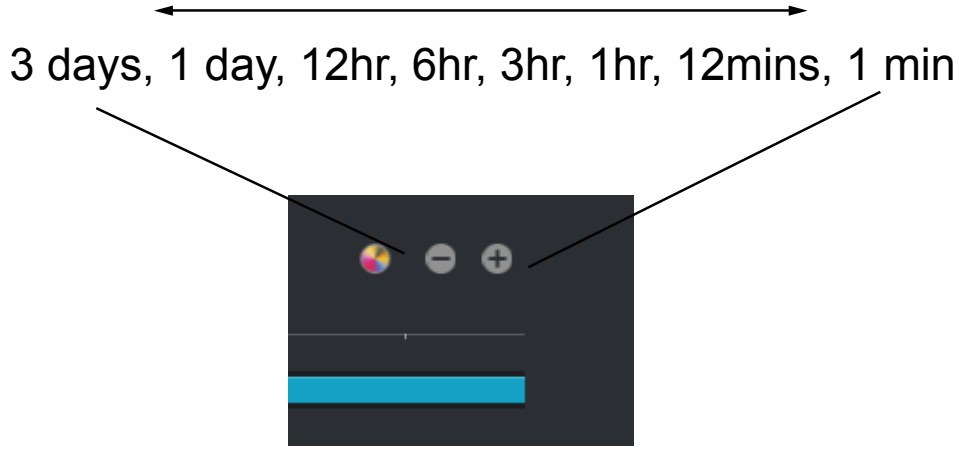


Blue: days with recordings.
Orange bottom line: Today.
White: days with no recordings.

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:

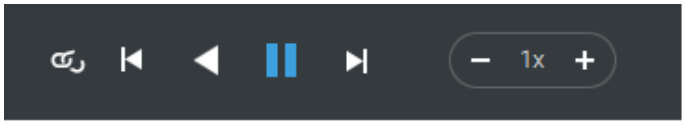


2. Playback control:

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.

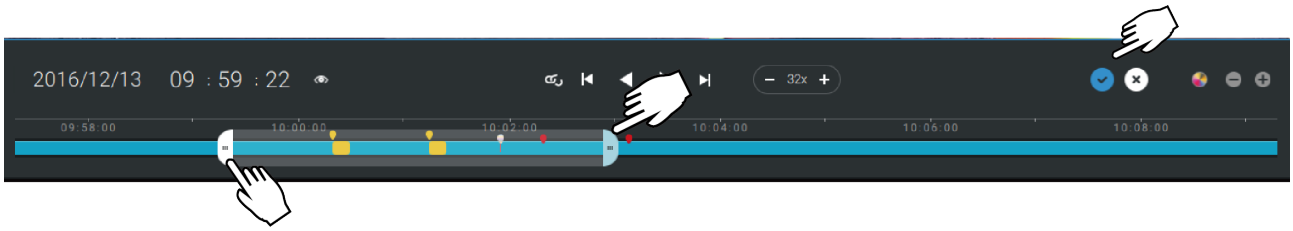
2-2. Frame by frame buttons: Click to move forward or backward to flick through the video frames. This may only display the I-frames.



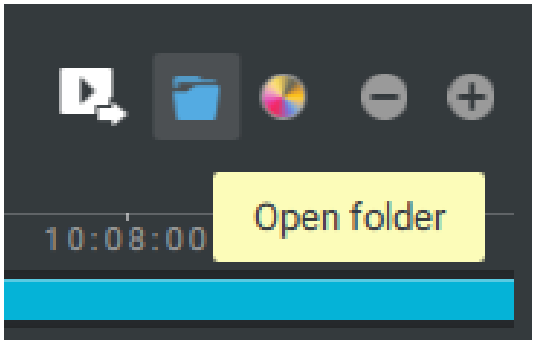
2-3. Forward playback and reverse playback: Click to view the video in the forward or reverse playback manner.

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.

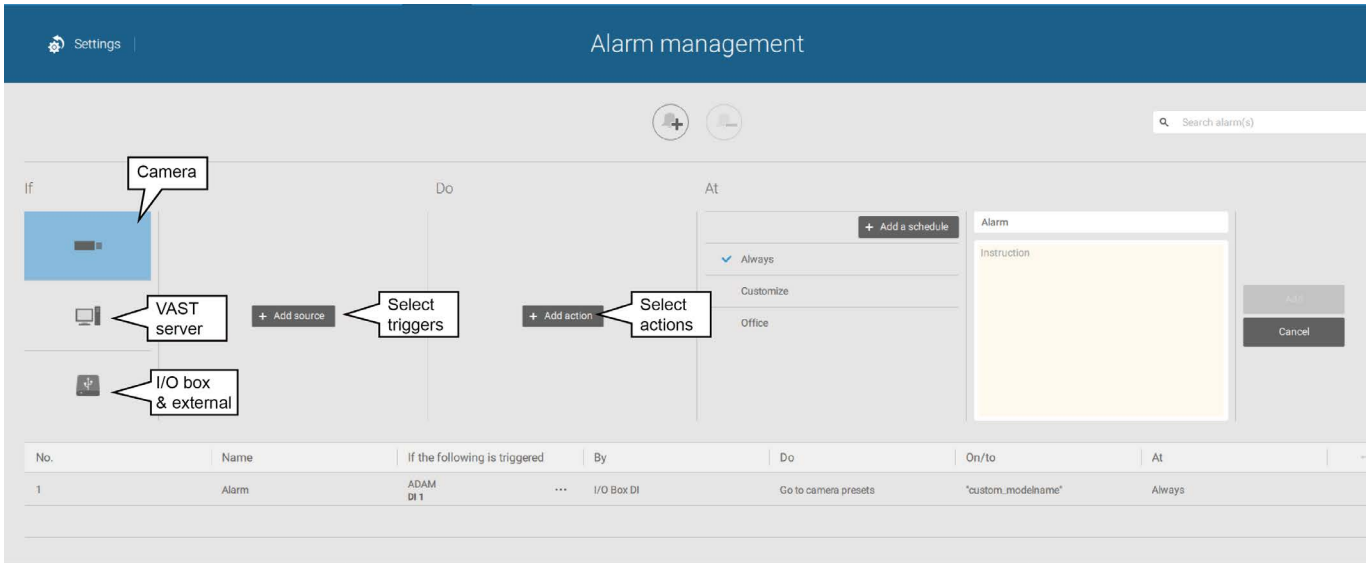


Depending on the length of video clips to export, it may take minutes to export. When the export is completed, a shortcut to the exported clips is shown. You may then open the folder where the clips are located.



2-2-14. Alarm

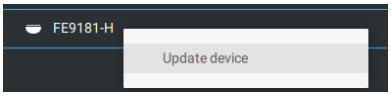
The Alarms can be configured to perform a series of actions when different events occur. Alarms can be used to automatically react to possible threats. For example, the VAST server can start a recording or send an Email notification when Motion detection is triggered.



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

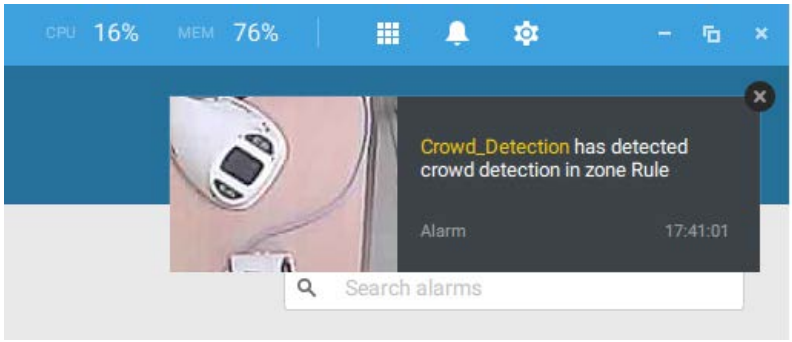
1. Camera triggers 

General			
●	Motion detection	●	IR (Infrared)
●	Camera DI	●	PIR (Passive Infrared)
●	Camera DO	●	Tampering detection
●	Temperature	●	Camera disconnected
●	Recording error	●	Stop recording
●	Video loss (Video server only)		
Smart VCA			
●	Line crossing (VCA)	●	Intrusion detection
●	Loitering detection	●	Face detection
●	Missing object detection	●	Unattended object detection
●	Crowd detection		
Trend 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.

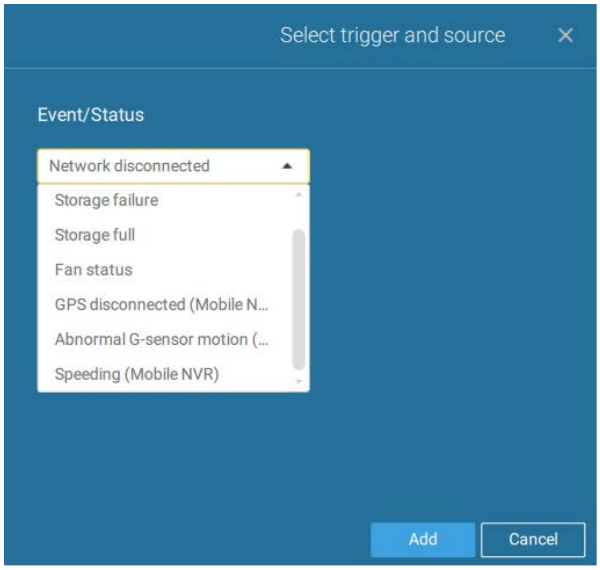
If a triggering condition is associated with event recording, an event prompt will pop up on the screen when a triggering condition is met. For example, the number of people exceeds a preset threshold in a Crowd Detection configuration. The sample prompt is shown below. The related footage can be played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

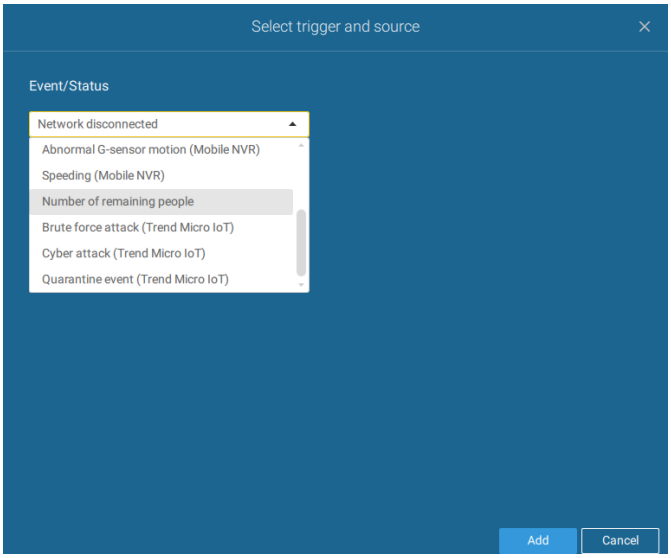


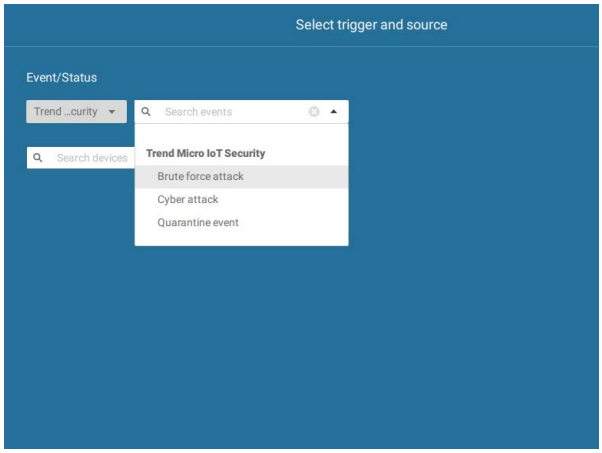
2. VAST server and NVR triggers

●	Network disconnected	These can be used to send maintenance notifications.
●	Storage failure	
●	Storage full	
●	Fan status	
●	GPS disconnected (Mobile NVR)	The GPS and G-sensor related options apply to the Mobile NVR that comes with the GPS and G-sensor. GPS can be used to track the speed and location of a vehicle, while the G-sensor can be used to detect abnormal impact.
●	Abnormal G-sensor motion (Mobile NVR)	
●	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 (Trend Micro IoT)	These can be configured as alarm triggers to notify the administrator that malicious attacks have occurred. Note that these triggers are available with cameras or NVRs that come with the protection of Trend Micro IoT packages.
●	Cyber attack (Trend Micro IoT)	
●	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.







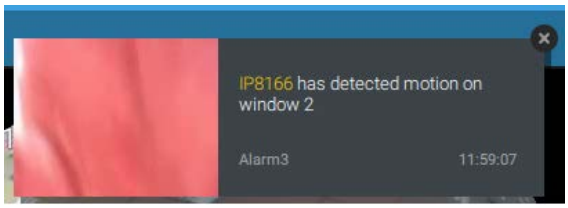
Note that the alarms will be received into the Alarm list window. The previous Alarm Search window is replaced by the Alarm list function.

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.

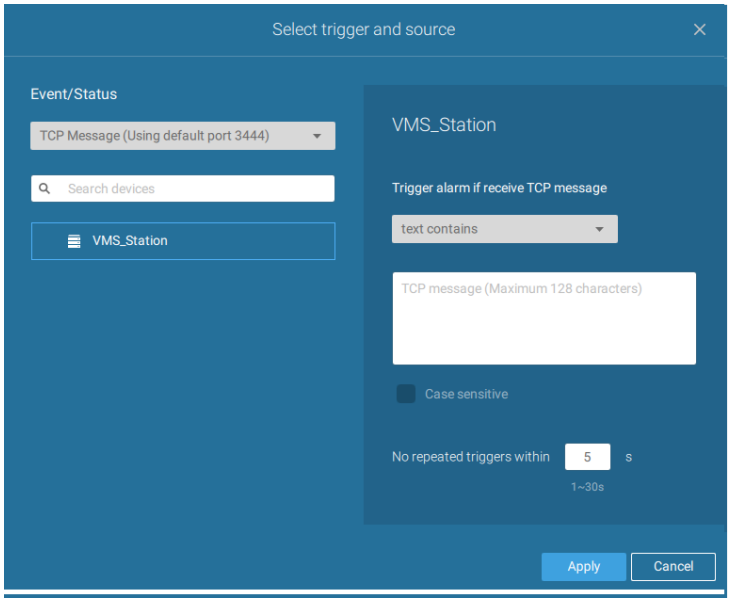
3. I/O box and TCP triggers 

•	I/O Box DI	This applies when an external I/O box is applied, e.g., Advantech's ADAM I/O box. 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.
•	I/O Box DO	
•	TCP Message	



To configure a TCP message trigger,

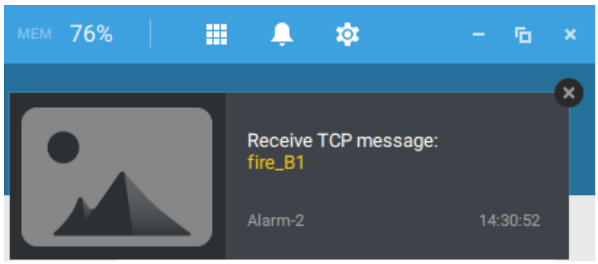
Select TCP message as a trigger type, and enter a description, such as a short term, for VAST to listen and analyze data packages.



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.



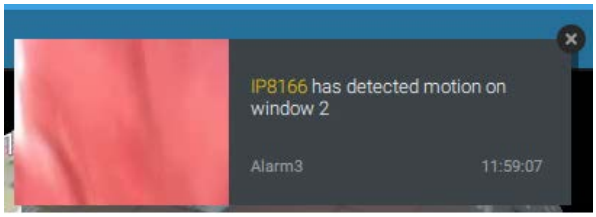
The available actions include:

•	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 Start to record video will record a video clip of the length of 10 seconds on the occurrence of an event. All 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.

The Send live streaming action will bring up a video prompt on the live view, 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.

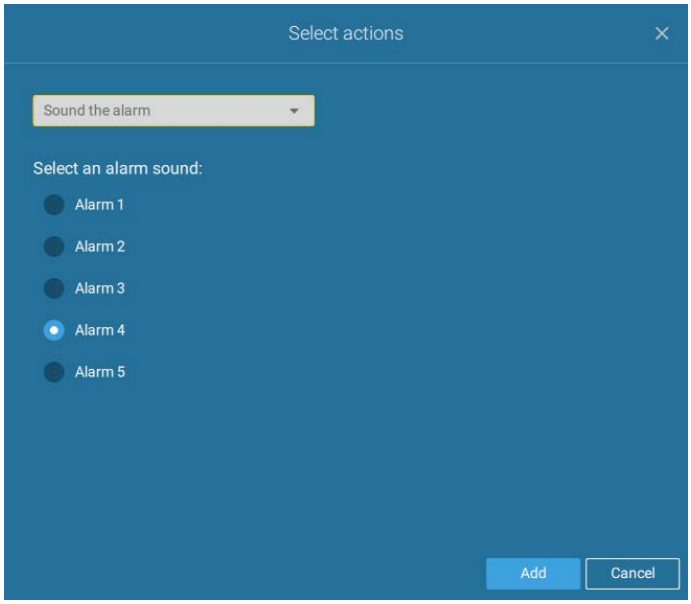
The VAST server automatically disables unavailable options. For example, when the DO option is selected, the cameras that do not support DO connections will be hidden.

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.

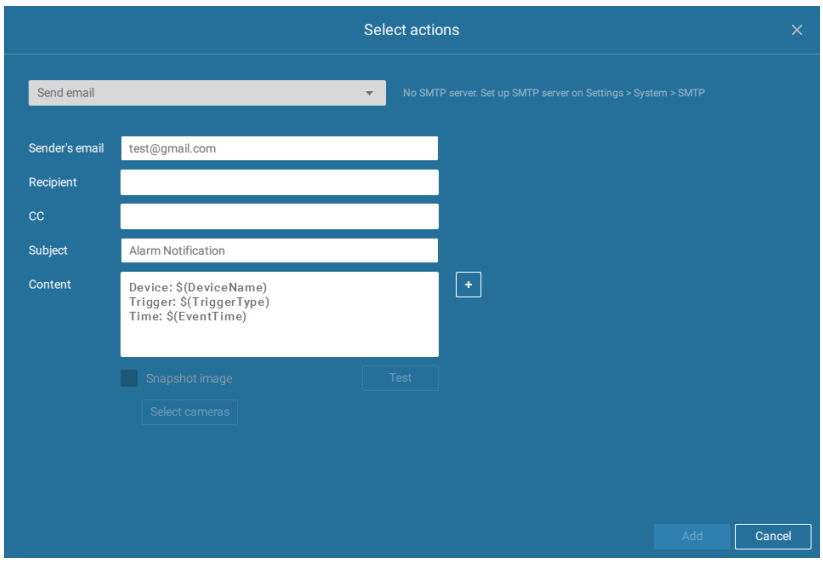
The Go to E-map opens a pre-configured E-map of where the triggering condition occurs. The user can then click on the camera icon on the E-map for an instant viewing.

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.

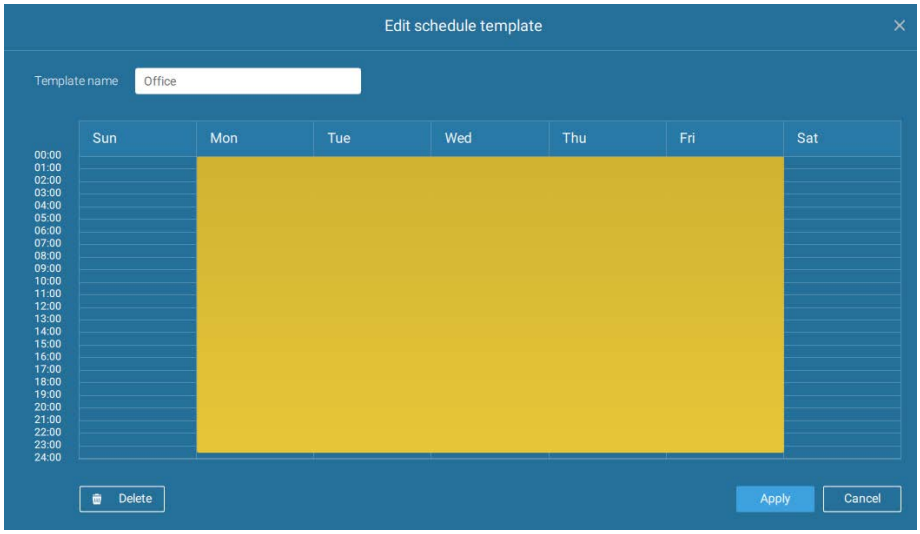
The Sound the alarm action provides 5 alarm sounds that will be sounded on the VAST client or server. Your VAST client or server should have spearkers for playing the audible alarm.



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

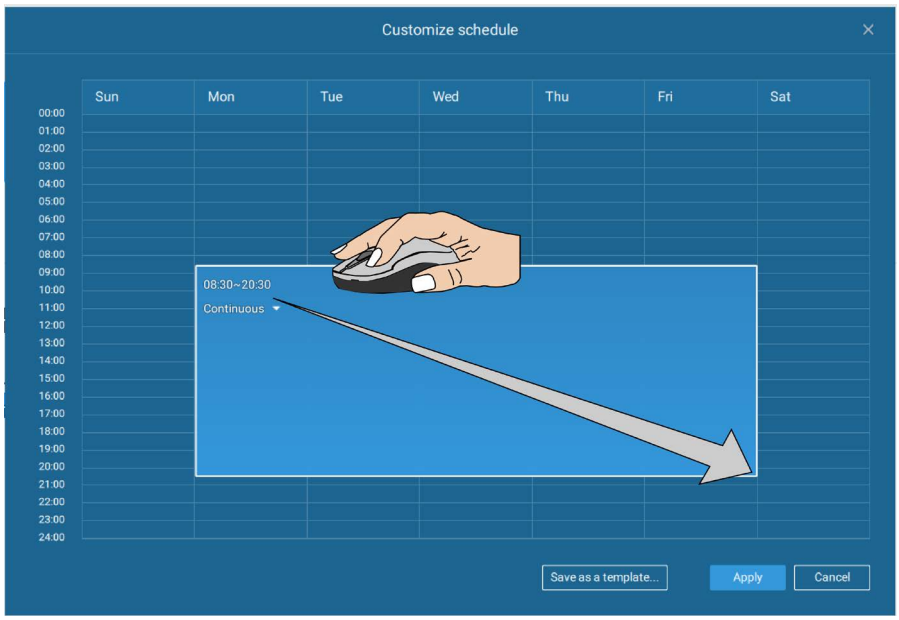


On the **Schedule** page, you can select to activate or de-activate alarm triggers throughout a specific timeline. For example, in some situations you can disable the alarm triggers during the office hours, and choose to enable the triggers only during the off-office hours.



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 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.

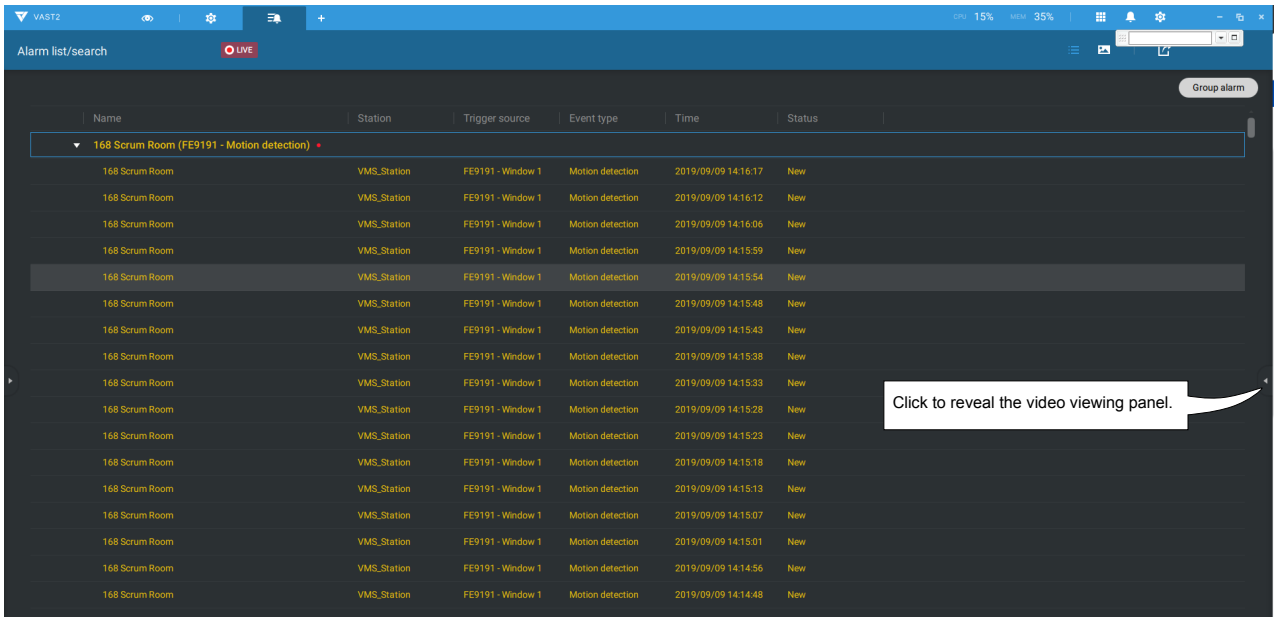
Enter a name and instructions for users to follow, and then click Add to complete the Alarm setting.

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

Group Alarm

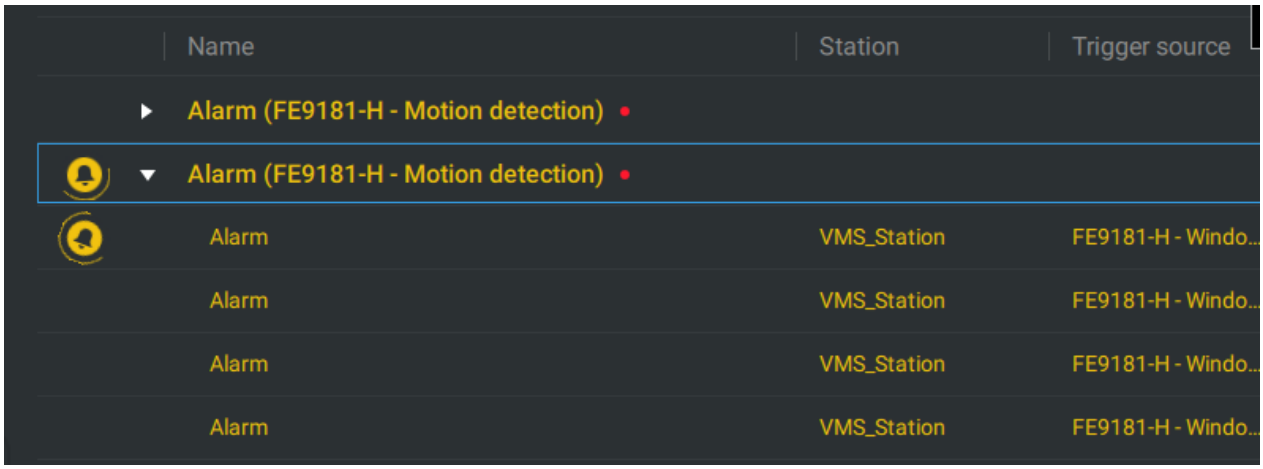
Multiple triggered alarms can be presented as group alarms. Alarms triggered by the same event type, and by the same camera can be grouped together. In this way, multiple similar alarms can be listed under one entry.

On the alarm list, click the Group alarm button to display the alarm group.

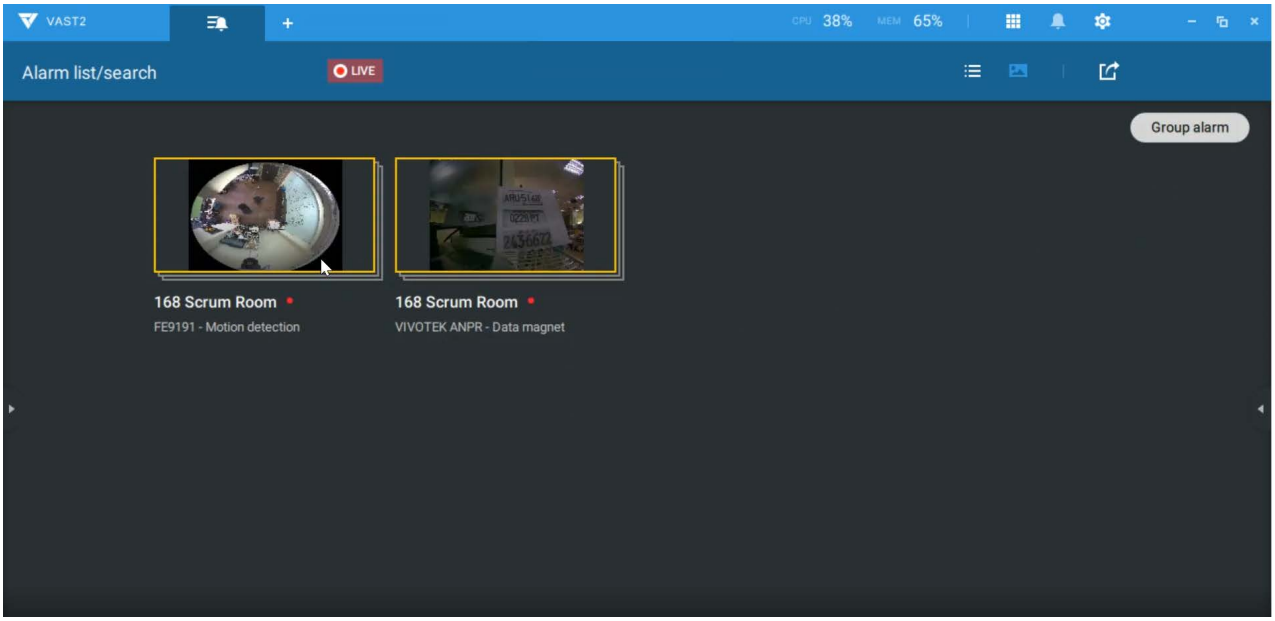


In the list mode, you can expand the right-hand-side panel. The video of the latest alarm will display.

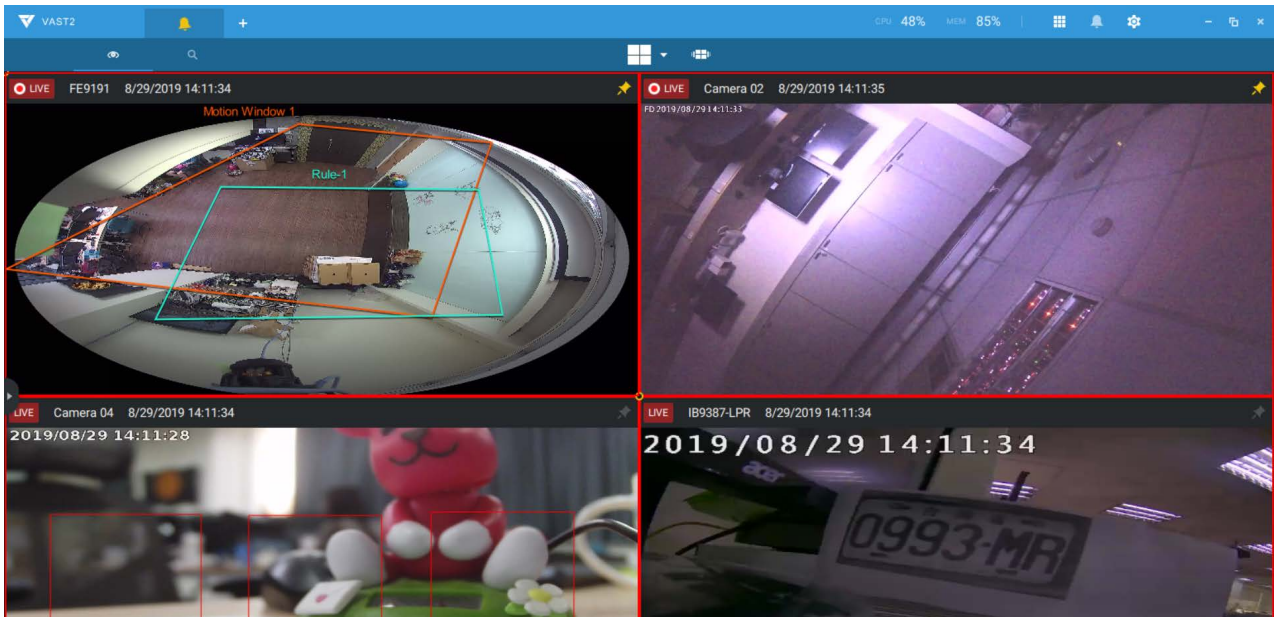
When the alarm-triggered action is configured as sounded alarm, you can mute all alarms in the group by clicking the alarm sound icon.



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.



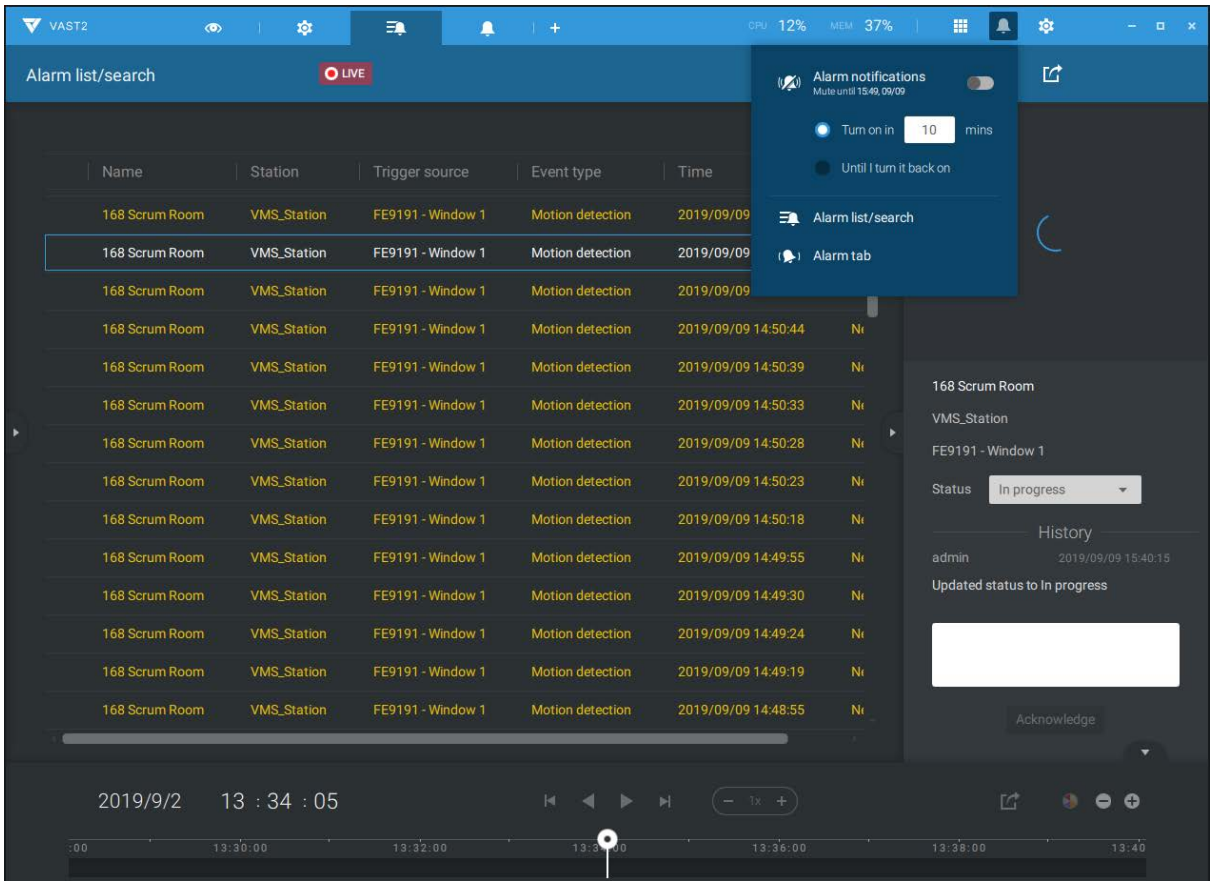
On the alarm playback view, use the thumbtack  button to freeze the current screen. If thumbtacked, the other incoming alarms will not affect the current screen.

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

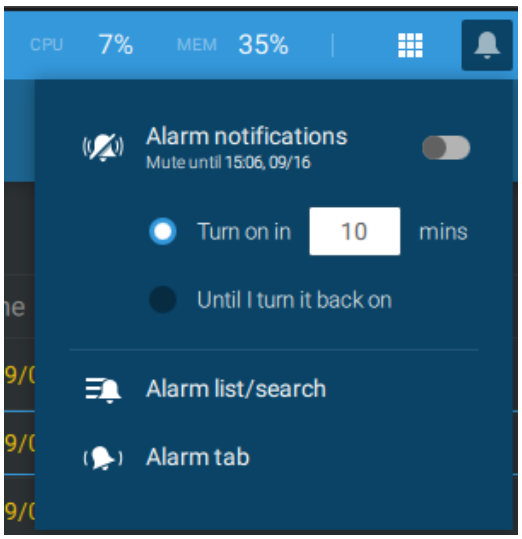
The alarm notification can be turned off by clicking on the Alarm tab. Use the slide toggle to do so. You can also select to let the notification automatically turn on after a configurable span of time. Enter the number in the mins field. The max. time span is 9,999 minutes.

The notification configuration is kept on the client computer.

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



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 button. 2 key functions are provided: Search by **POS** transaction, and Search by **Bookmark**.

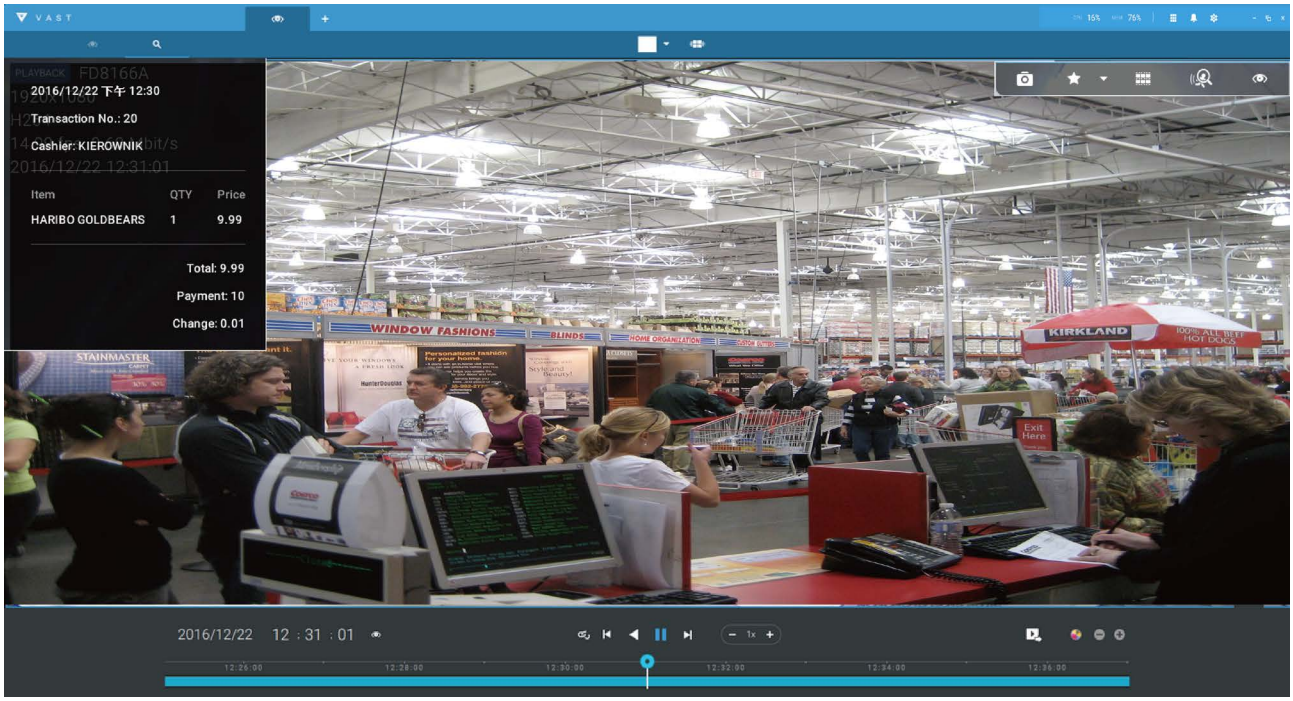
1. **Search by POS transaction:** The VAST station can collect coordinated database information from a POS machine. This function provides access to the video clips associated with the sales record on the POS machine. Details of transaction can be listed on screen so that a manager can see the live view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

To search the POS-related recordings,

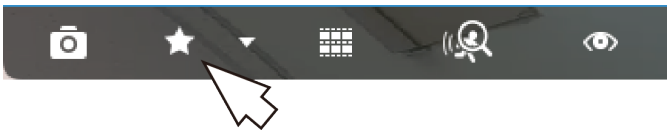
2-1. Select the VAST station which the POS machine is connected to (via the Settings > POS configuration).
2-2. If you know the approximate time of occurrence (bill void, content adjusted, shortage of products, and other frauds), use the calendar to select a time span.
2-3. Select a POS machine, if there 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.

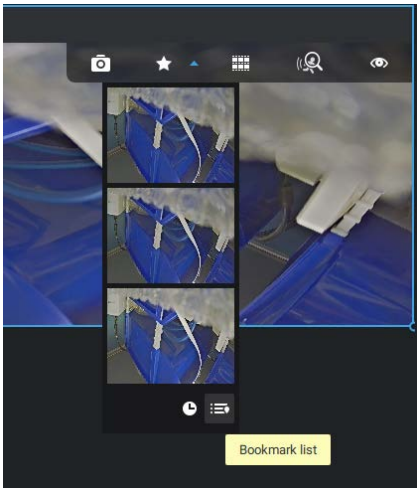
NOTE: The Alarm search panel is replaced by the Alarm list function. The Alarm list is accessed from the top tool bar.

2-7. Click on any of the search results. Details of the transaction will display along with the recording of the time of occurrence.

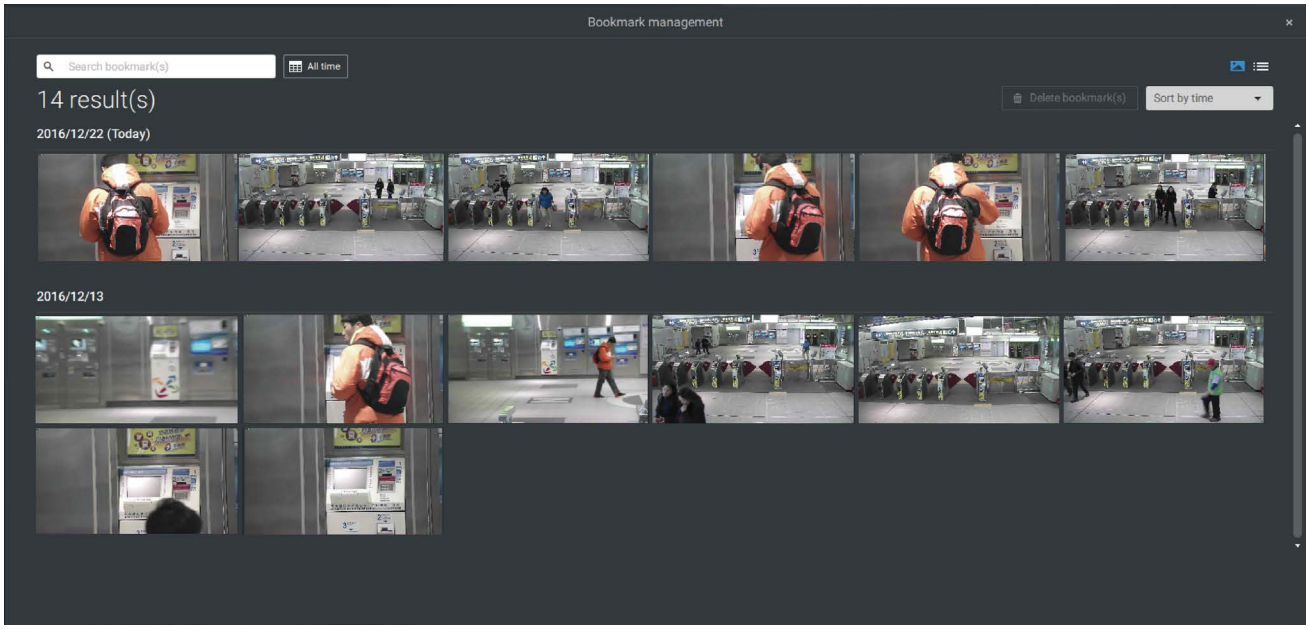


2. Search by Bookmark: Bookmarks are manually created when users review recorded videos in the Playback mode. Each bookmark comes as a 10-second video clip.





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 user-configurable detection area from the recorded videos. **Smart search** is available in the **Playback** mode.

Click to select a camera view cell. Click on the Smart search button  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 Detection feature.

To use Smart search,

1. Use the date and time selectors to specify a time span on which to perform the Smart search. If preferred, you can tune the Sensitivity, Continuous detection for exclusion, and the Interval between search results. The Continuous detection option specifies the length of occurences that an event must last longer than the configured threshold to be considered as an effective occurrence.
2. Draw one polygon with multiple mouse clicks to include areas where activities of your interest occurred. Double-click to close a polygon.

3. Click the Search button.

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

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 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.

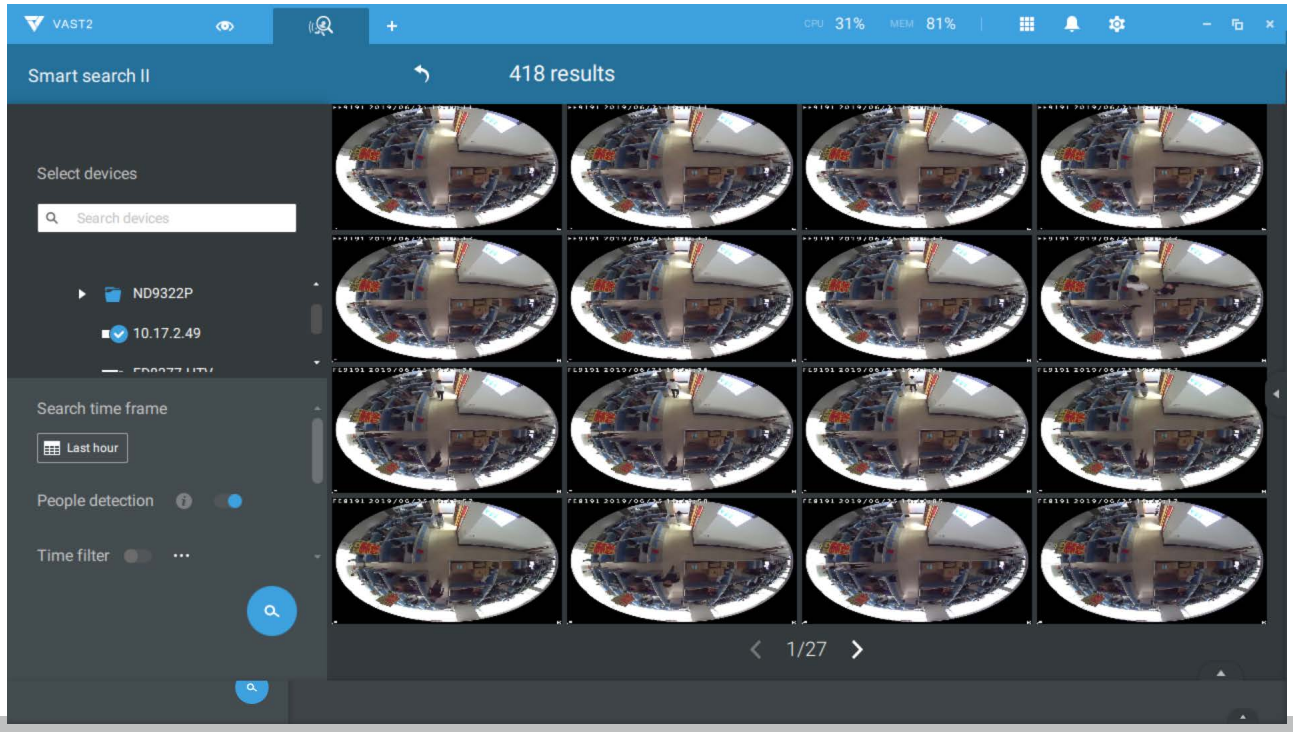
Search parameters:

Time frame	Use the calendar tool pane to specify the time span within which the activities in scene will be searched.
Human detection	Human detection enables the display of the alarms detected via the human silhouttes algorithm. This can be used to filter out video analytics alarms that are not related to human activities.
Sensitivity	Configure the sensitivity for the detection of the activities in scene. Low for near scene, high sensitivity for long distance scenes.
Continuous detection for exclusion	If the detected motion persists for longer than the time threshold, the motion will be counted as a detection result.
Intervals between search results	The intervals for defining and revealing the detection search results.

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.

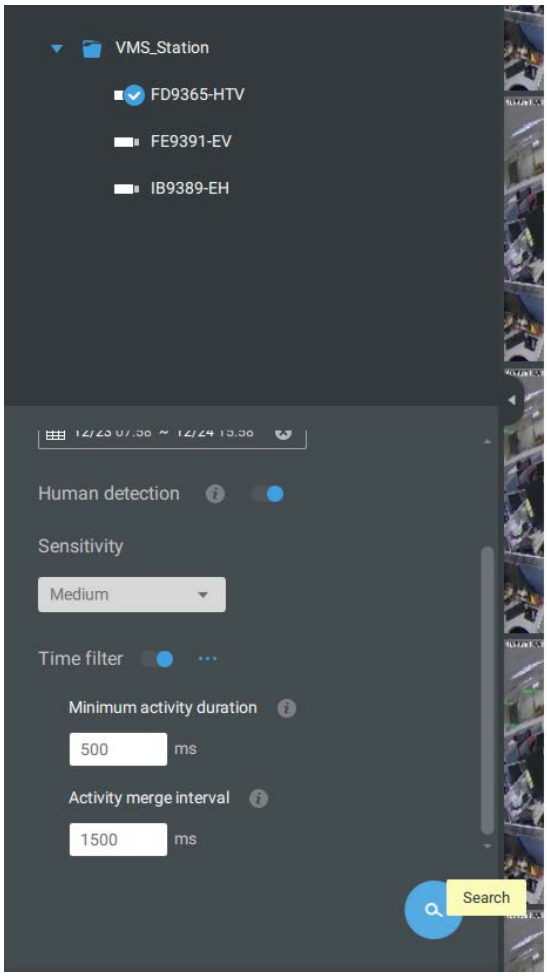
Note that unless interrupted, the playback continues with all detection zone clips, by continuing to the successive clips.



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

1. Faster search: Metadata is saved with videos coming from cameras running Smart Motion 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. Human 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 polygon.

Note that the Smart Motion detection areas must have been configured on each camera before the Smart search can take effect.



You can specify the time span, Human detection, Sensitivity level, and time filter parameters in a Smart Search II panel.

Below are the statuses of the Smart Motion detection polygon:

Normal

Motion window (normal)

Selected by a mouse click. You can click on the delete button to remove a configured window.

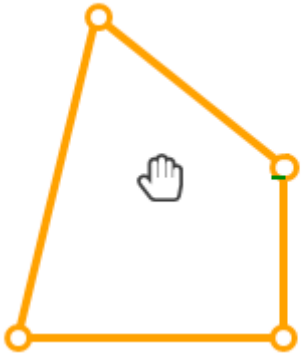
Motion window (focus)

When motion is triggered in the window.

Motion window (trigger)

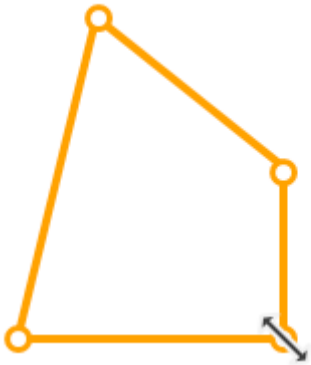
When moused over. You can edit the end points.

Motion window (hover on area)

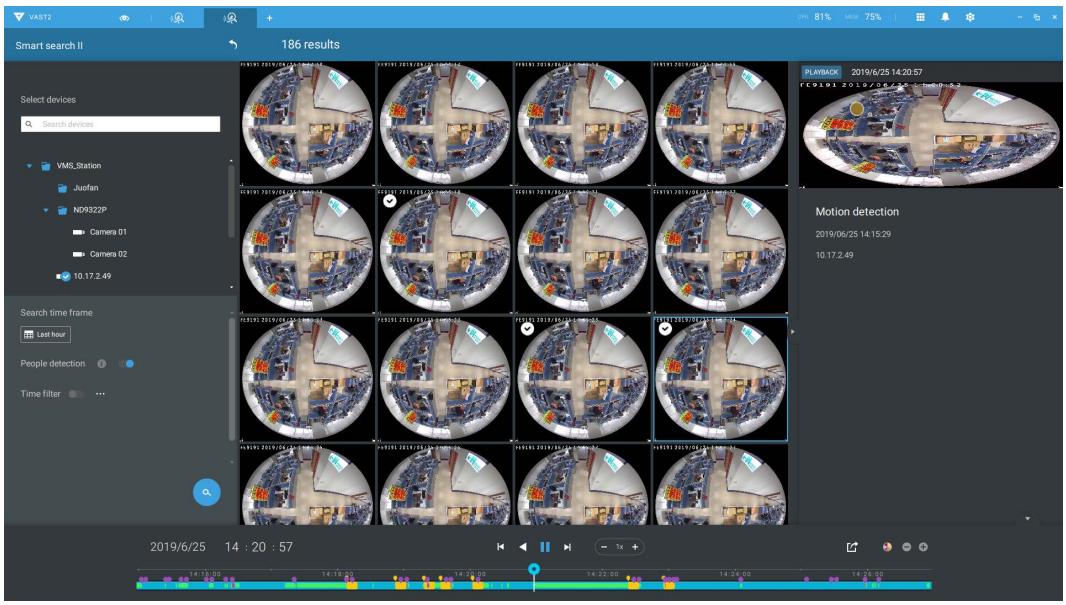


Click and drag the end points to edit the coverage of the motion window.

Motion window (hover on point)

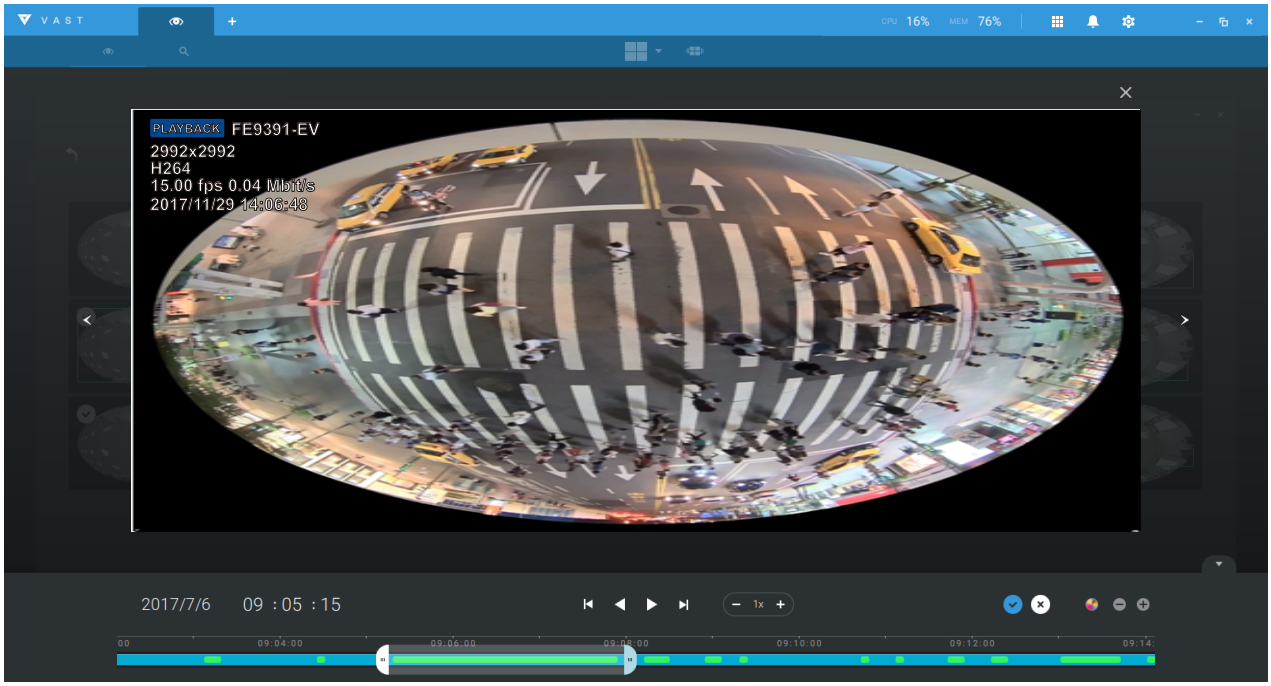


5. You can then click to open any clip of your interest. Each marked event clip will be indicated by a lighter color on the time line. Select and double-click on a video clip, and then right-click or select the bookmark or snapshot functions from the upper-right.



6. 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.

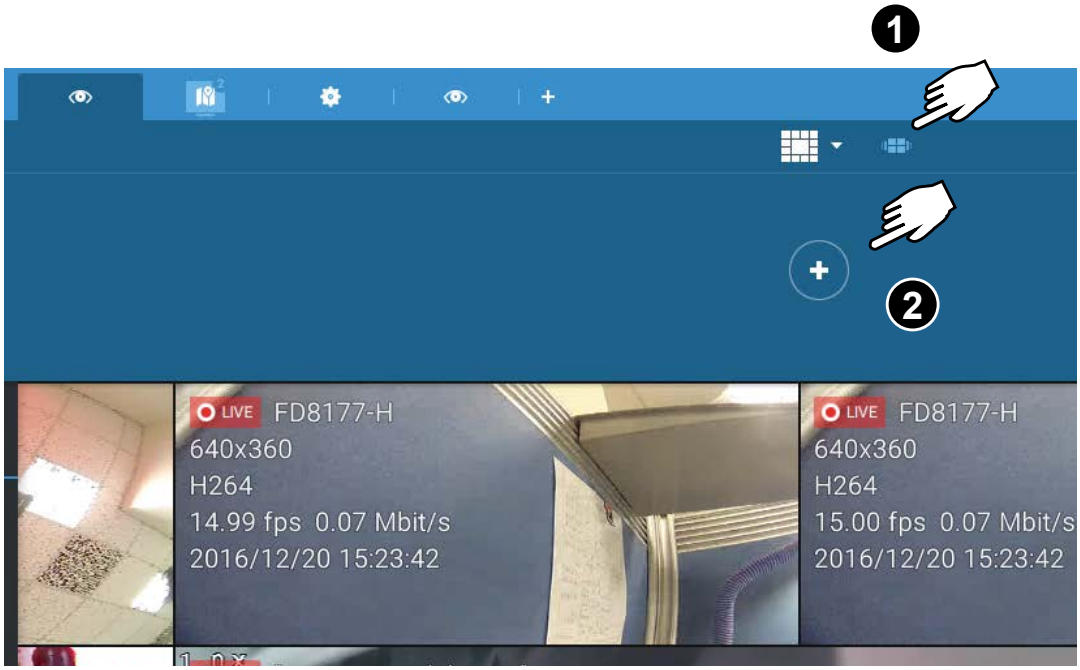


2-2-17. Tour

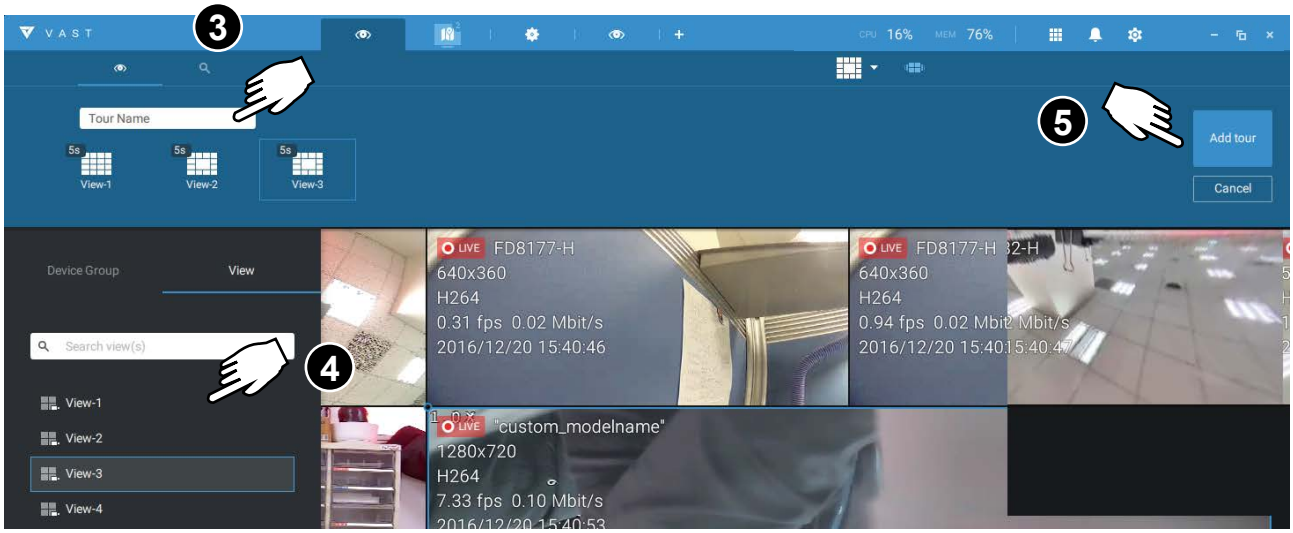
A tour can be configured to consecutively display multiple views. A tour allows users to quickly glimpse through many view cells in a timed pattern. As a tour can contain multiple views, you should design and configure camera views before configuring a tour.

To configure a tour,

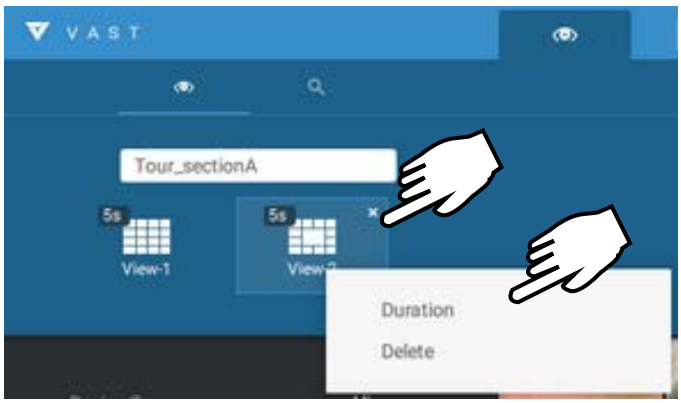
1. Click on the Add a camera tour button.
2. Click the Add button.



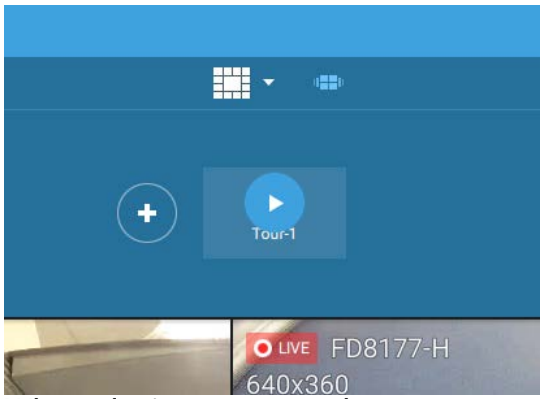
3. Enter a name for the tour.
4. Single-click to select a view. Select multiple views each by a single click.
5. Click the Add Tour button.



The default for the duration of the disaplay 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.



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.

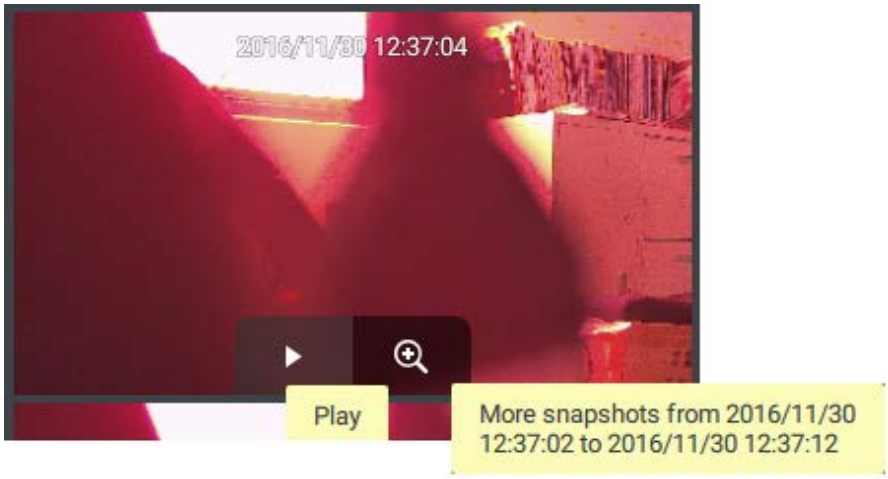
To use Thumbnail search,

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.

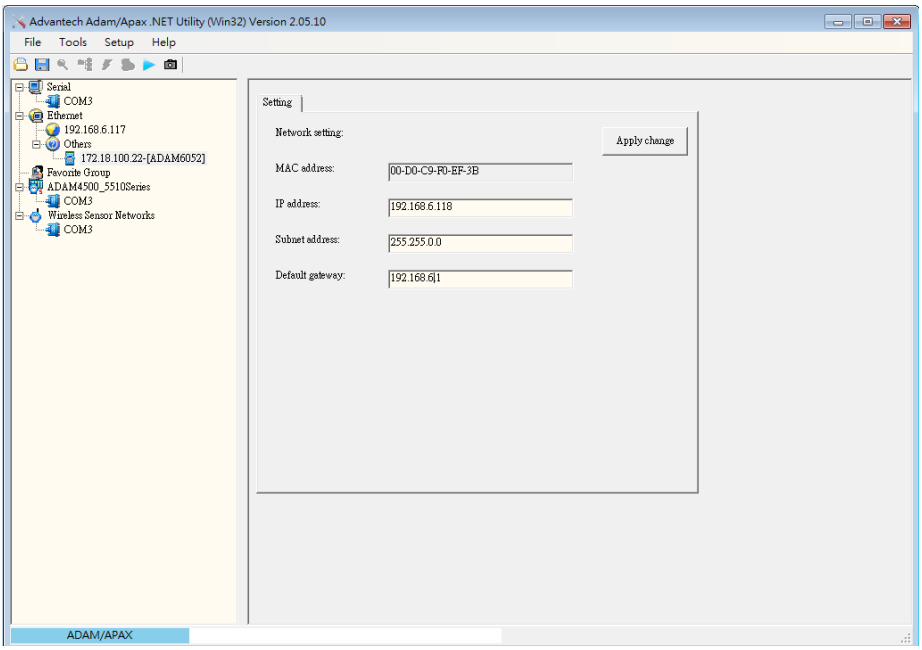
When you find an event of your interest, you can play that video clip and use the export function on screen to output the evidence. You may also place a bookmark on the timeline.



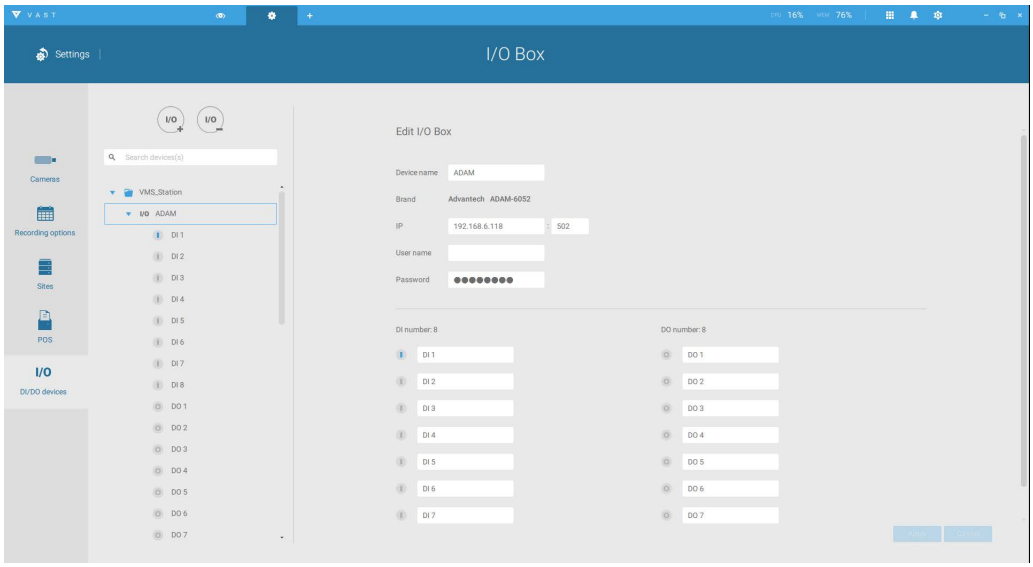
Chapter 3 Applications:

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.



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

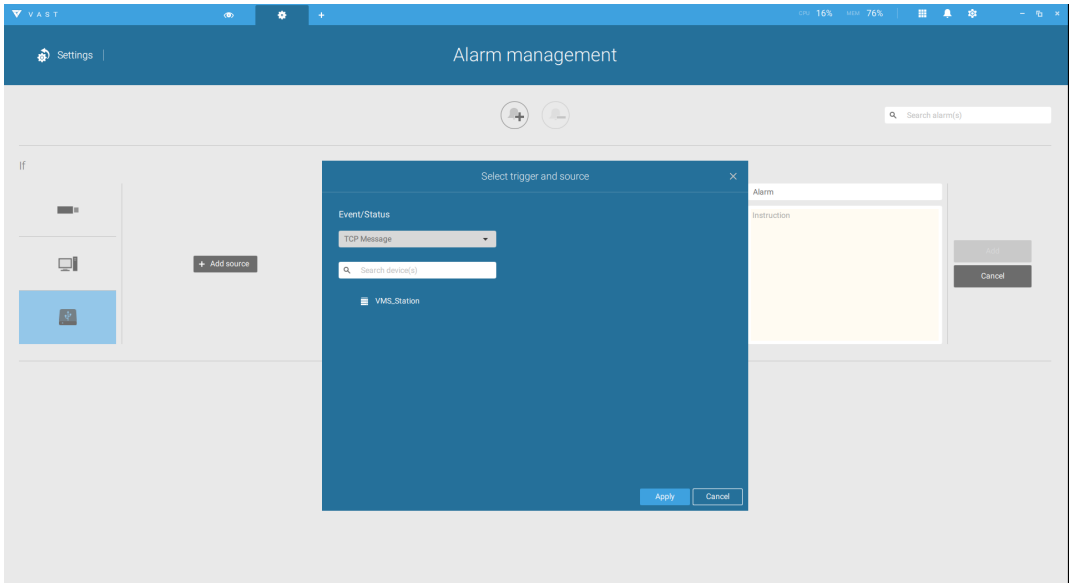


Enter the I/O box's IP addess and credentials, and select the correct model name from the pull-down list on the right. Click the **Apply** button to proceed. The current I/O connections are also displayed on screen, such that the status is displayed when DI pins are connected to detection devices.

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

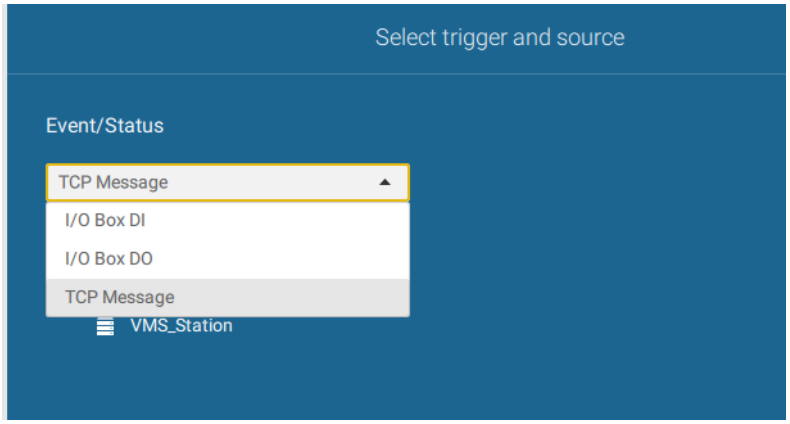
Enter the Settings > Alarm window. Click the Add alarm button on top.

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

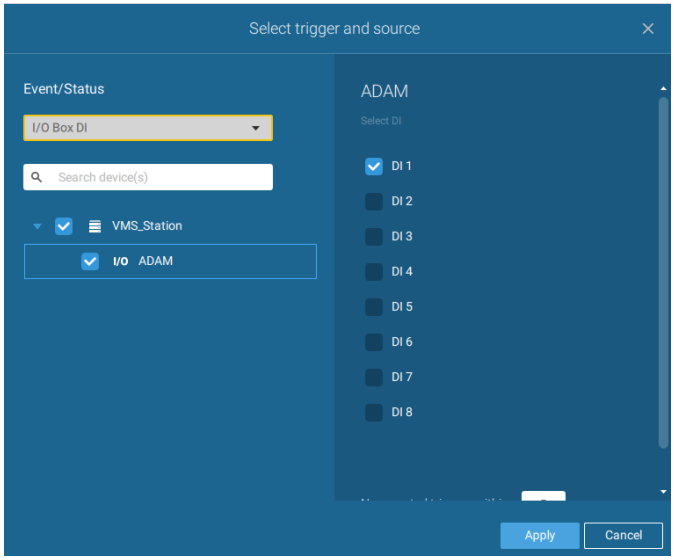


The **Select trigger and source** window will prompt.

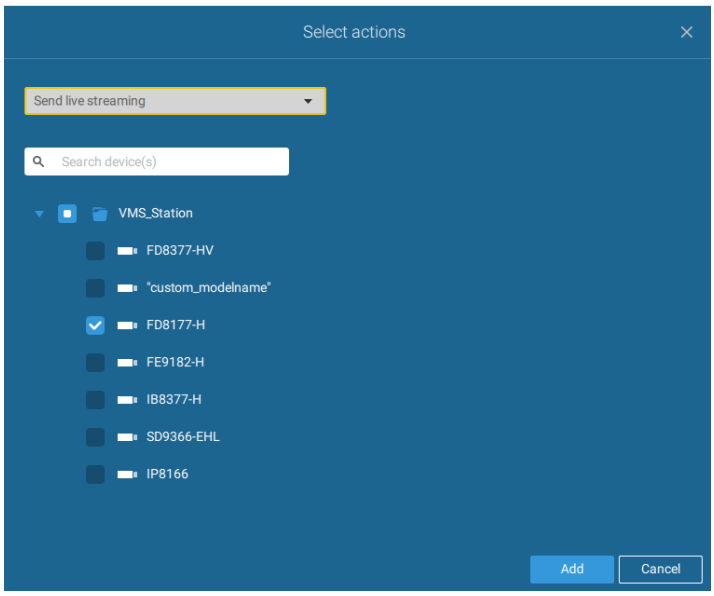
Select either the I/O Box DI or DO as the triggering source.



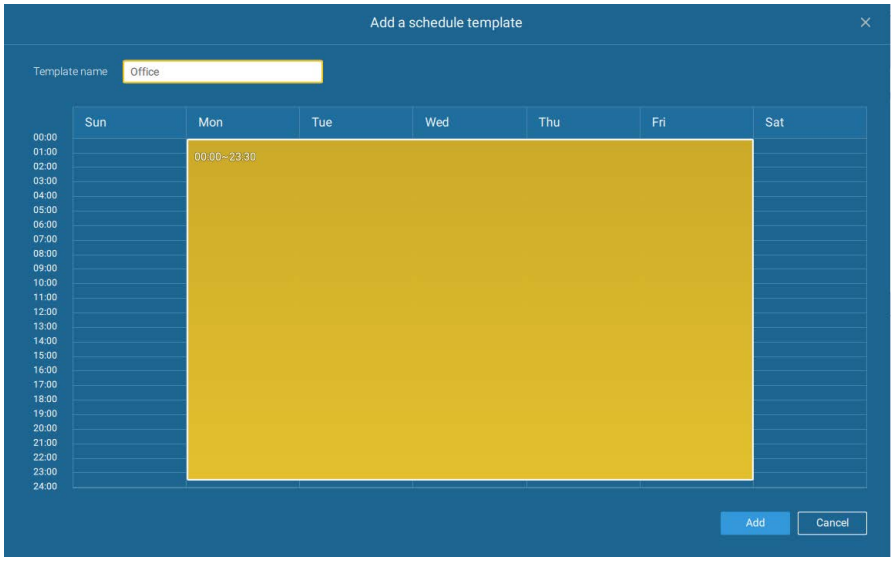
Select one or multiple DIs as the triggering source and click the **Apply** button.



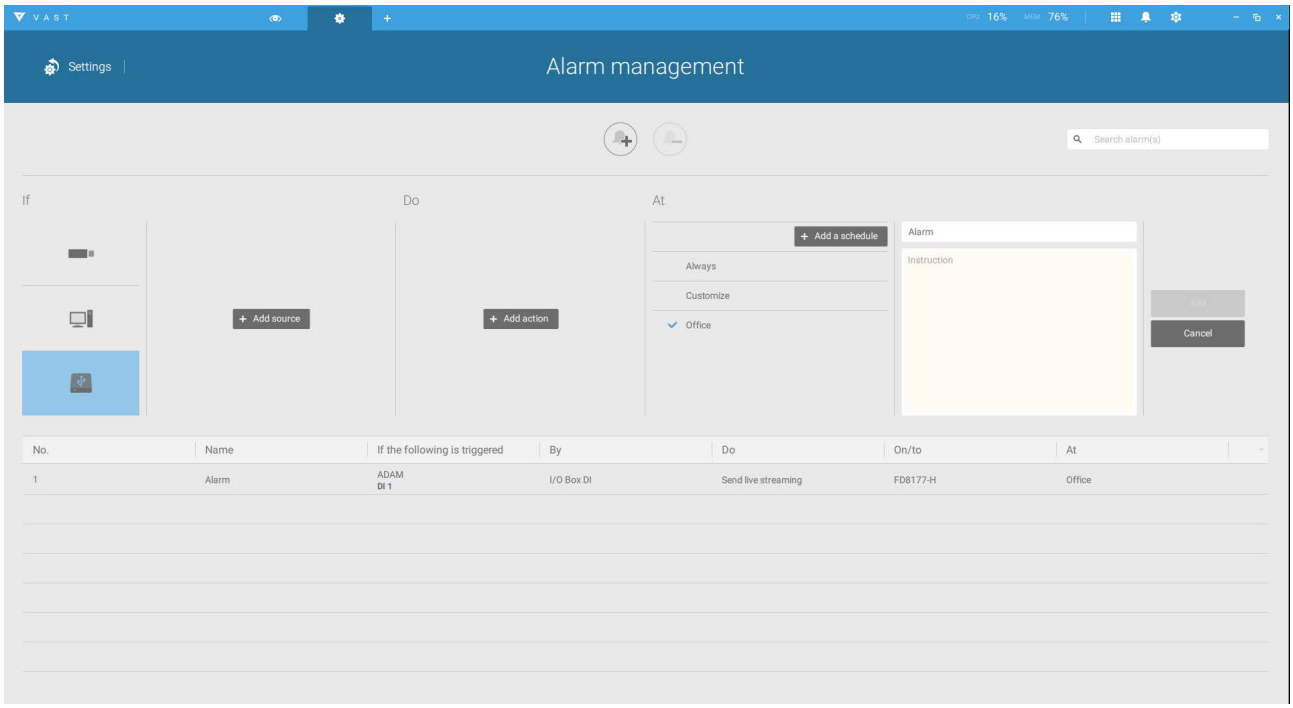
Click Add action + Add action, and select a corresponding action, such as sending live streaming, record videos, trigger a DO, sending an HTTP request, or sending an Email. When done, click the Add button.



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

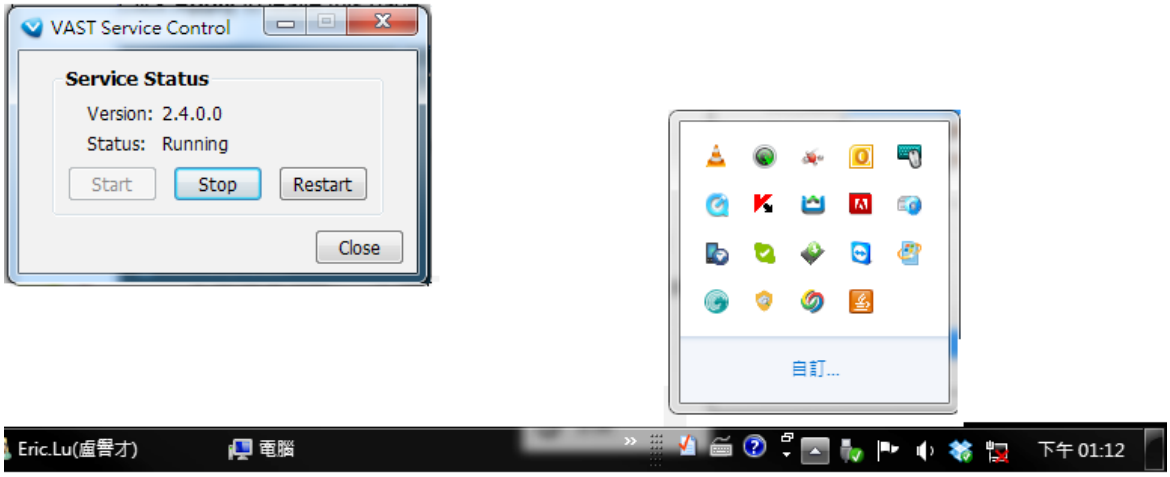


Enter a name for your Alarm, and add description for your configuration, e.g., "intrusion detected on the front door." When done, click the Add button. The Alarm configuration takes effect immediately.



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

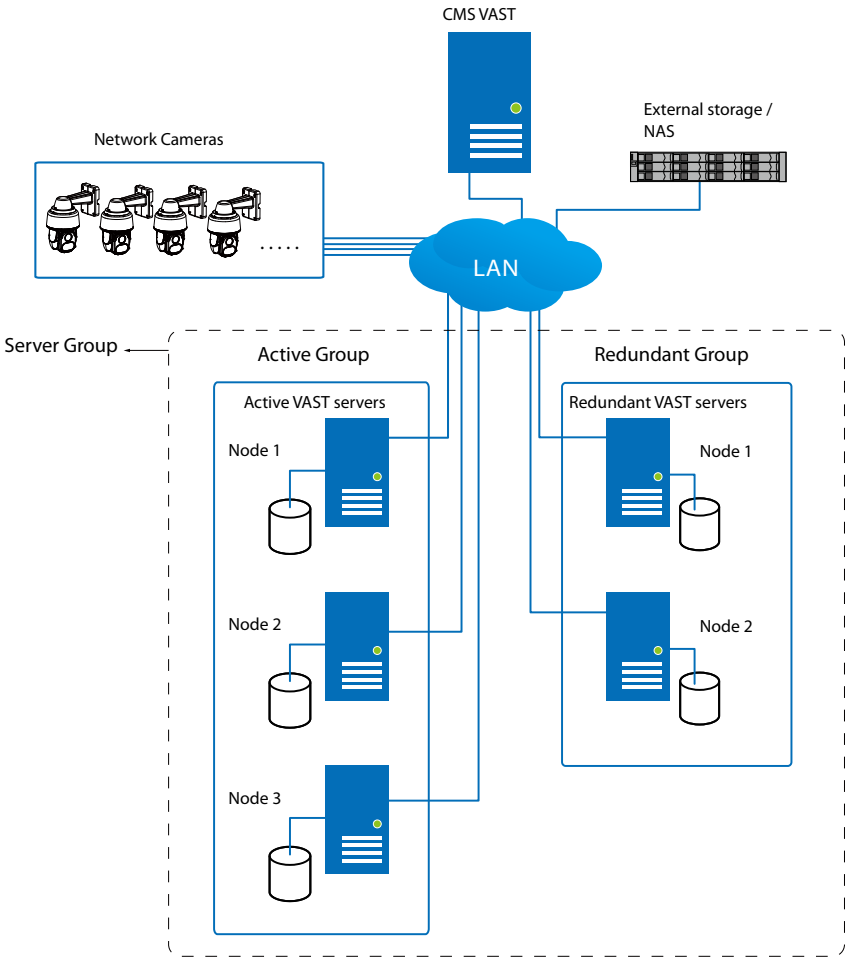
VAST2 servers can be configured into two groups: Active and Redundant. The Active group performs daily recording and monitoring tasks, while the Redundant group acts as the standby servers. In the event of server failures, the Redundant group becomes active, and takes over the recording task.

The Redundant server group configuration consists of the following:

1. One VAST2 server designated as the **CMS** (Central Management server) VAST central management server.
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 connection 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.

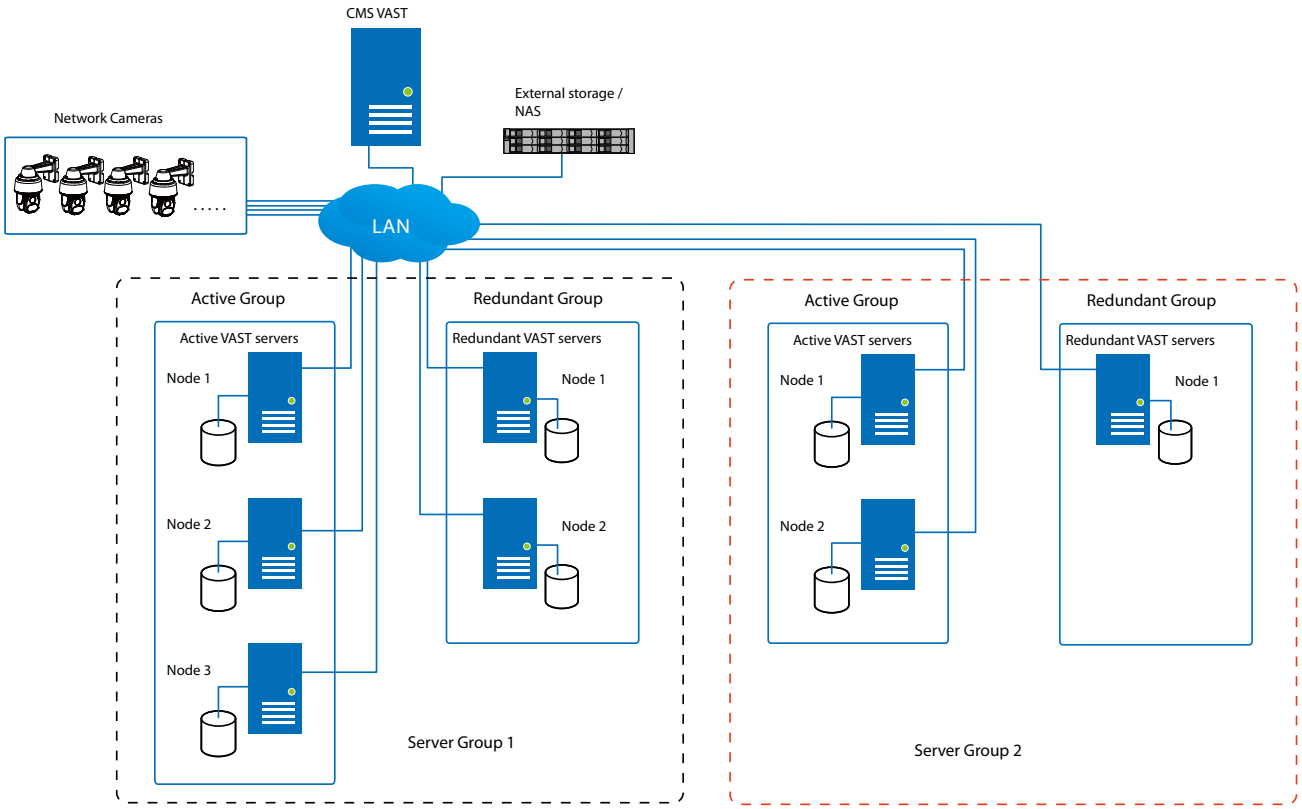
1-1.	CMS server is where the **Failover** configuration takes place.
1-2.	CMS continuously polls to check the hearbeats to monitor the statuses of all Active and Redundant servers.
1-3.	CMS regularly backs up the configurations on Active servers.
1-4.	CMS assigns redundant server(s) to the takeover of 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 install the CMS server at a high up-time environment, such as on a VMWare configuration.

2. **Active** servers: Active VAST servers are the work horses that perform recording and monitoring tasks.
3. **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 server to have an equivalent or higher processing power than the Active servers. The same applies for the storage volume and write performance.

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

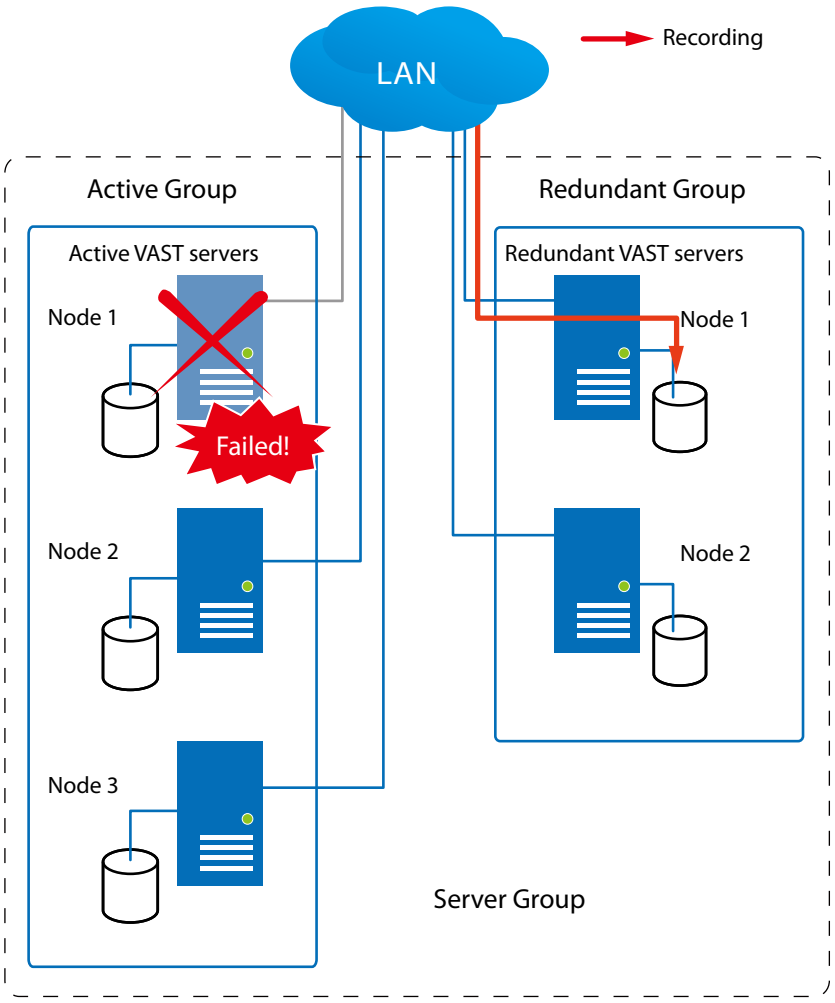
The conditions during the failover are illustrated below:

Multiple Active and Redundant groups can be created.

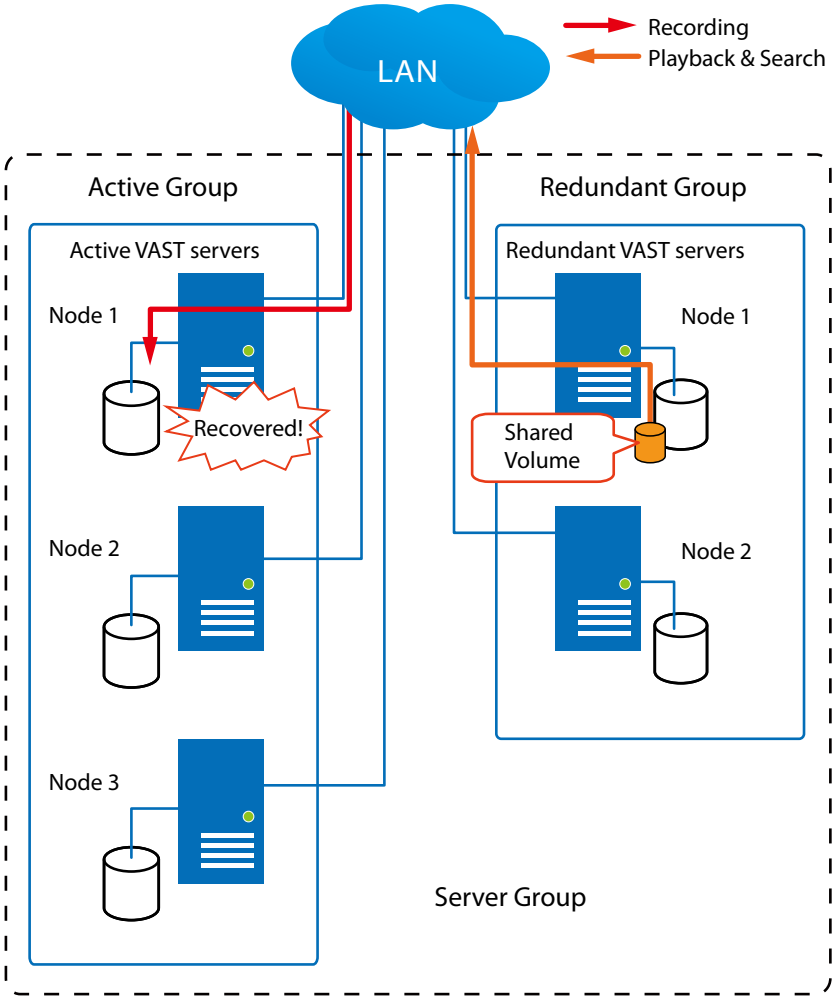


Each Redundant server can serve as the backup for ONE Active server. Depending on the number of the Active and Redundant servers, if the number of failed servers exceeds the number of Redundant servers, the failover will be abandoned. For example, if 2 Active servers failed, and there is only 1 Redundant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

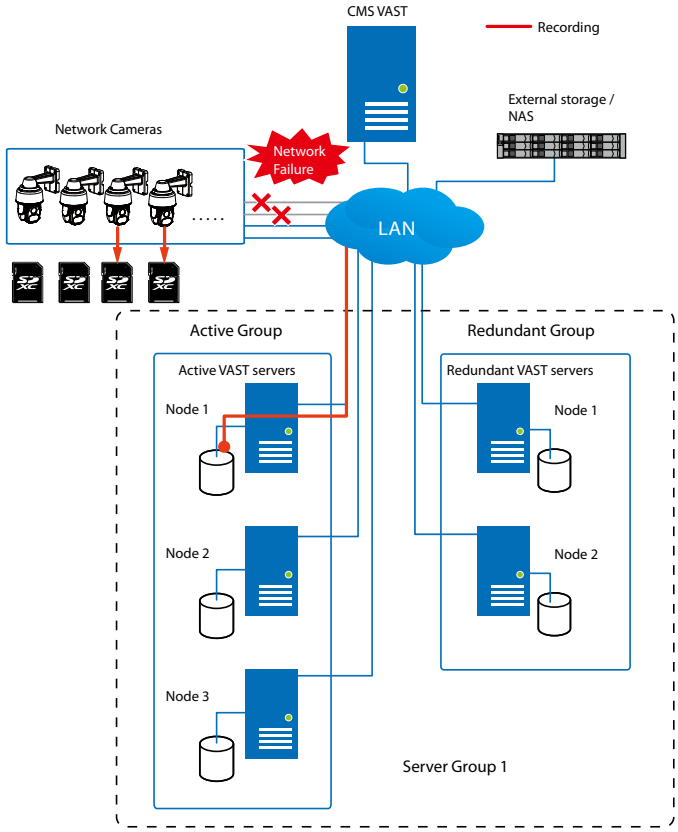
In the event of a server failover, a VAST2 server in the Redundant group takes over the recording task. Note that depending on the network environment, the takeover can take up to 5 minutes.



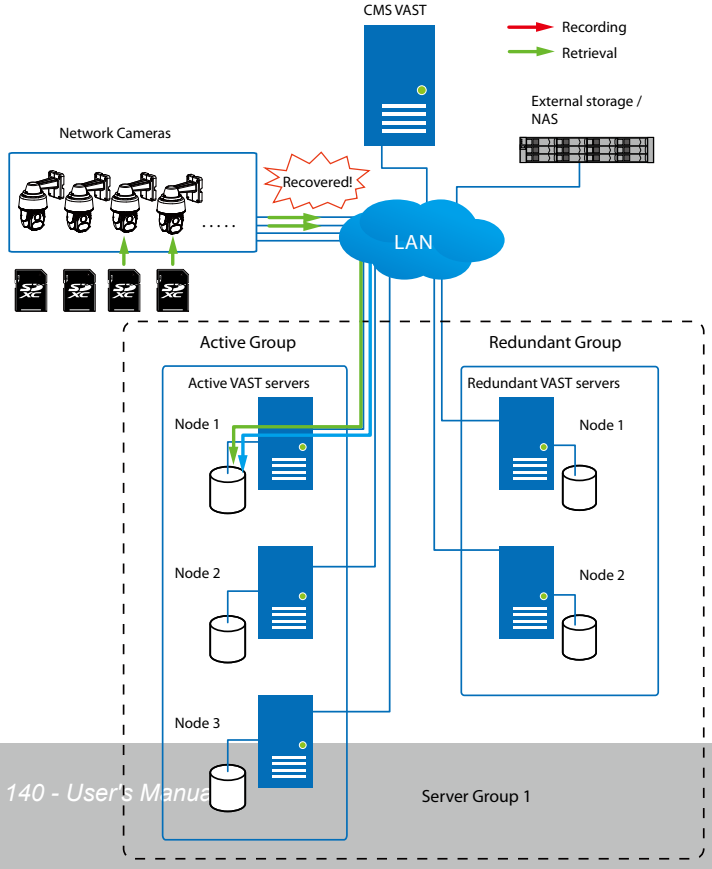
Once the server in the Active group is restored to normal operation, and a CMS server requests for the recordings and data occurred during the time the active server failed, the requests will be fulfilled by a shared volume on the redundant server. Due to the concerns with network bandwidth and processing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



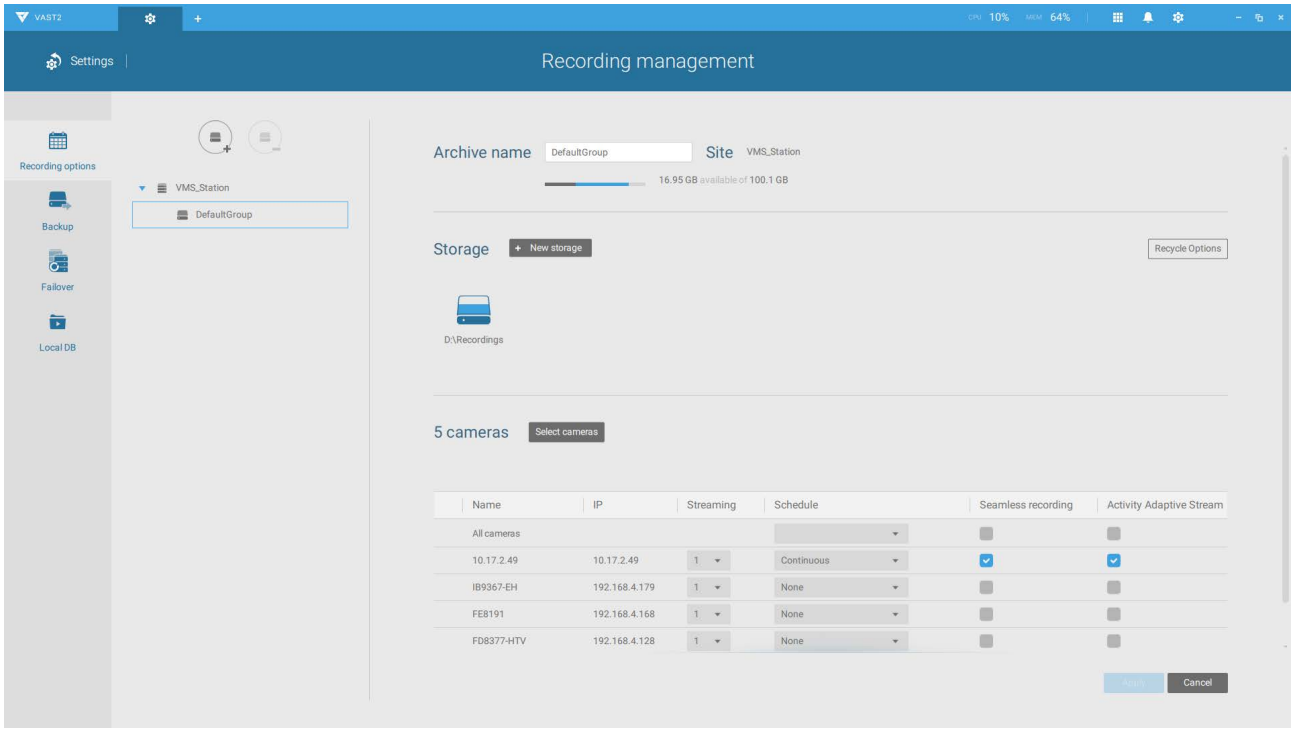
In terms of network failure, the VAST2 configuration supports Seamless Recording. For cameras equipped with an SD card, video is recorded to the SD cards in the event of network failure. Of course, the camera must be powered by a secondary power source, such as a DC 12V input. In cases such as the only 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.



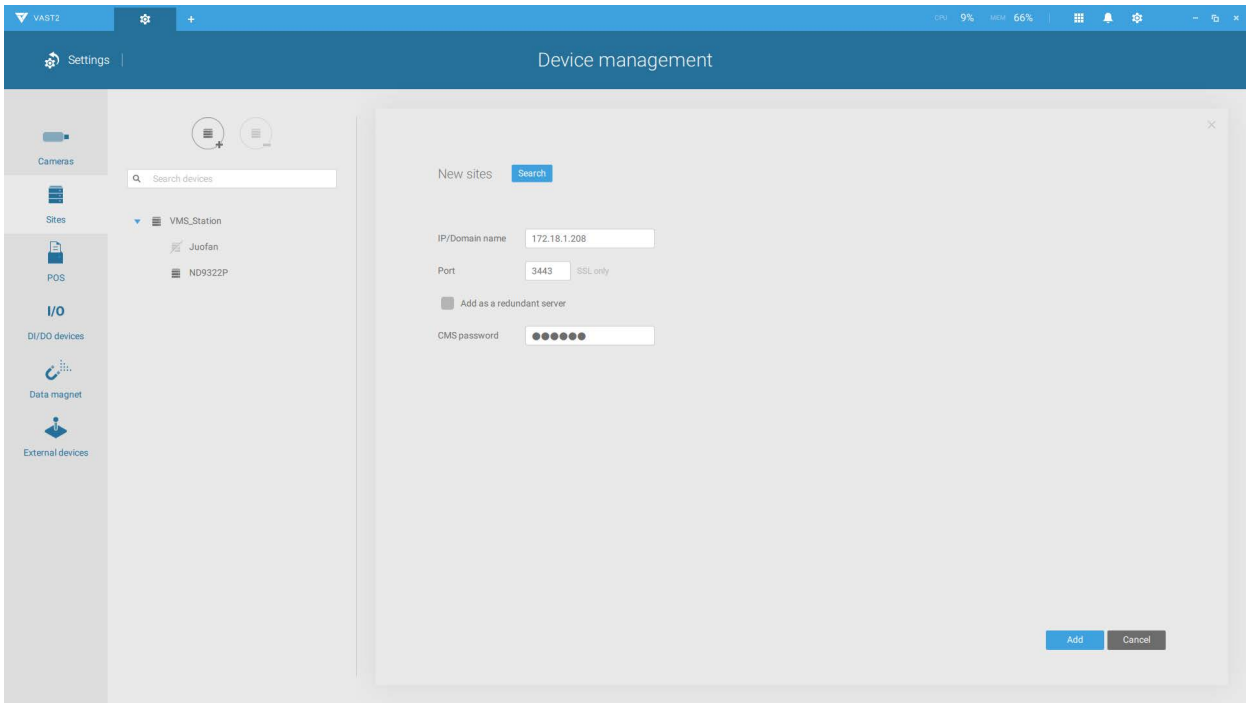
To enable Seamless recording, find the associated option in Settings > Recording options, and select the Seamless recording checkboxes. Camera models that support the Seamless recording option will have it listed.



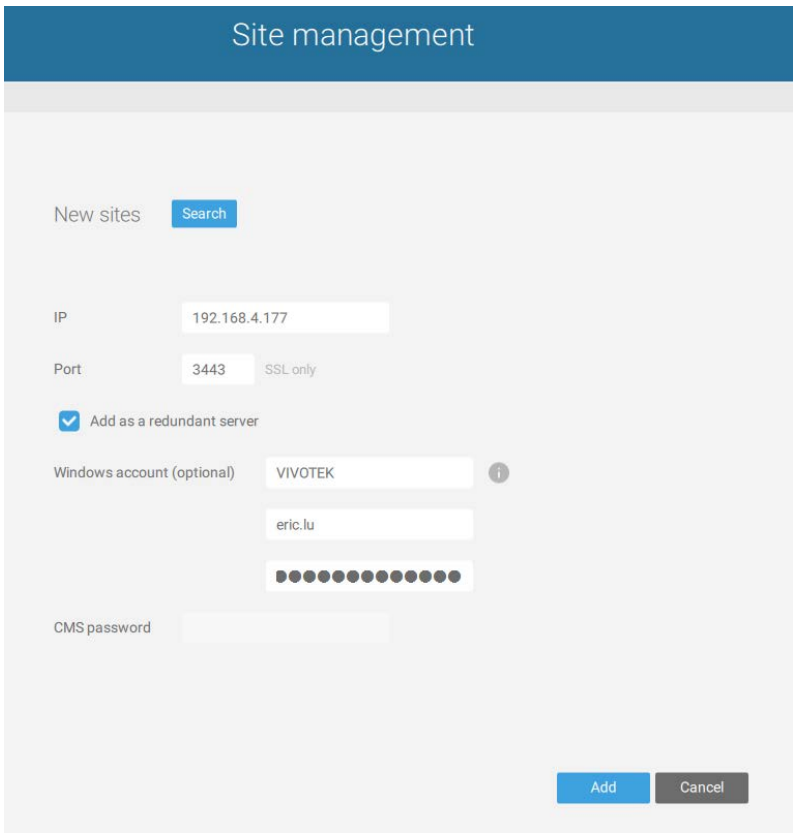
Failover Configuration Process

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

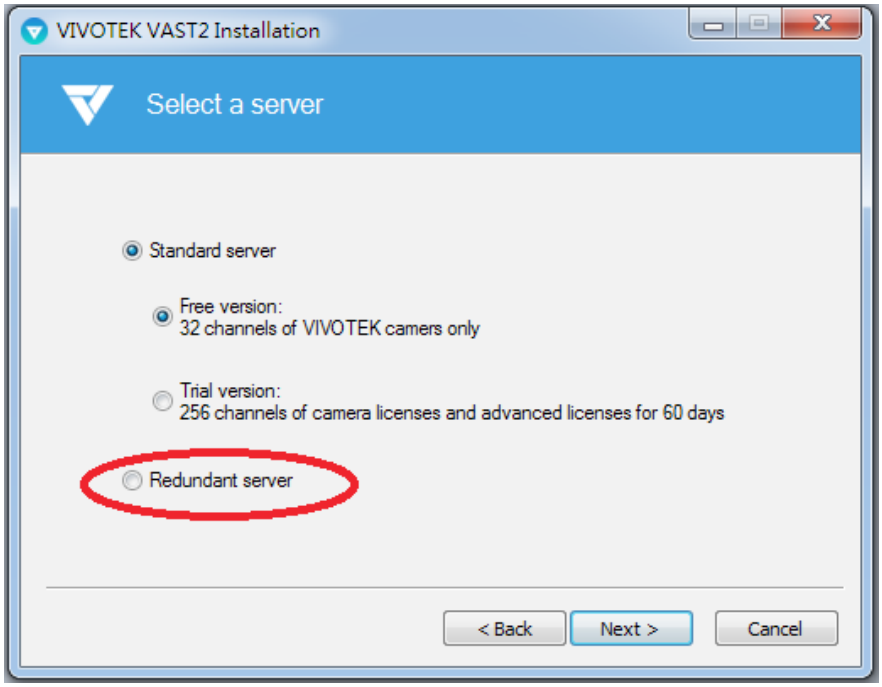
- If you are adding a Redundant server, select the "**Add as a redundant server**" checkbox.
- If you are adding a server without selecting this checkbox, it will be considered as an Active server.
- When adding a Redundant server, you will need to provide a Windows account 802.1x domain user name and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



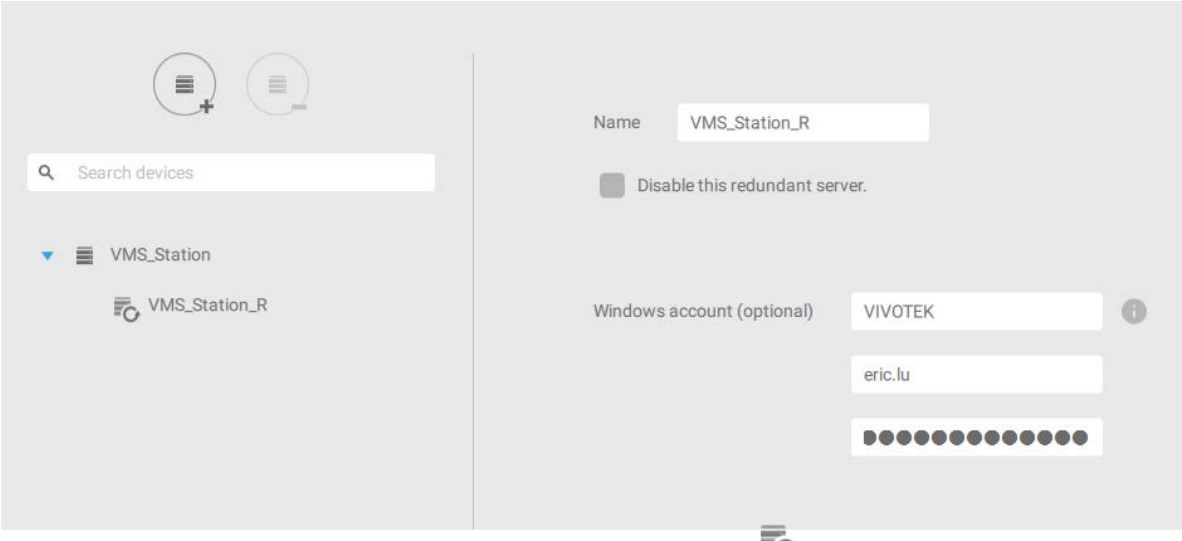
When the "**Add as a redundant server**" checkbox is selected, enter the name of your Windows domain and the user credentials for a full access to the Redundant server.



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



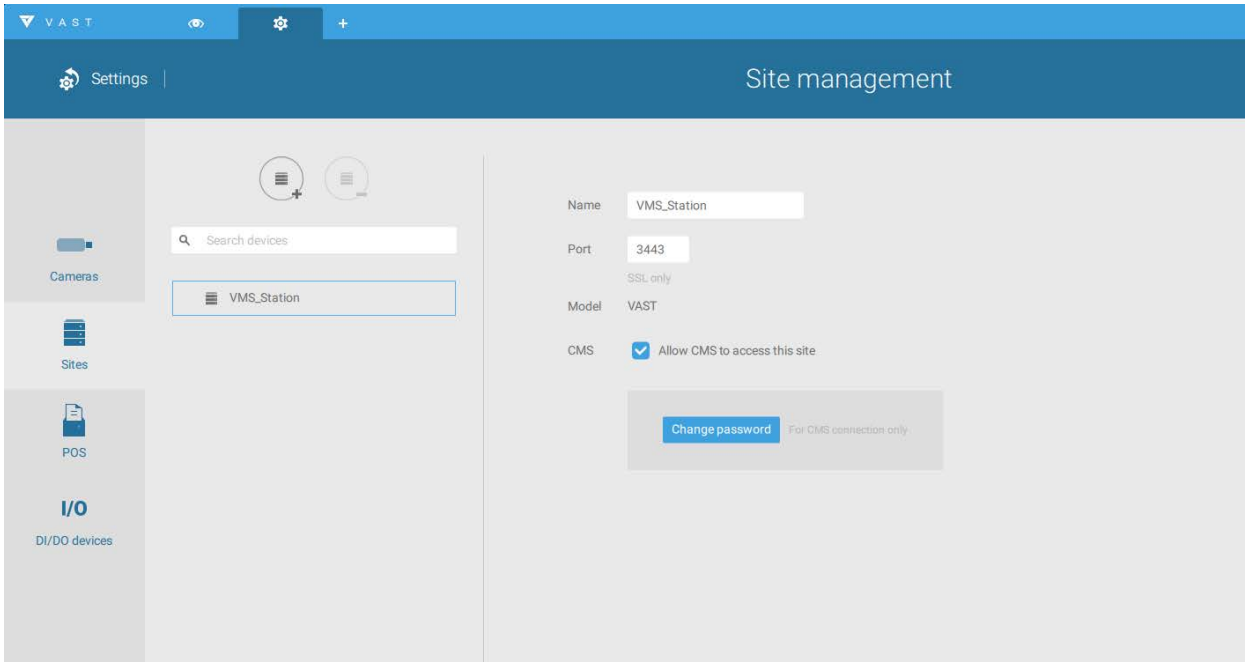
When a Redundant server is successfully added, the server will be listed under your VMS station.



A Redundant server comes with an associated icon,  .

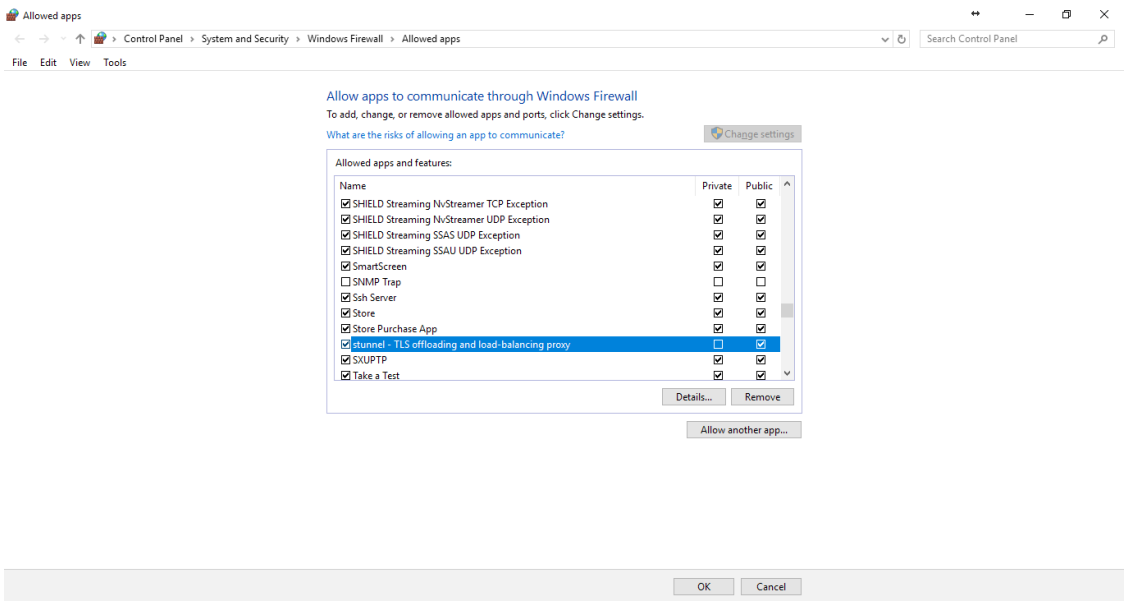
An Active server must have a CMS password configured for the hierarchical configuration.

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.



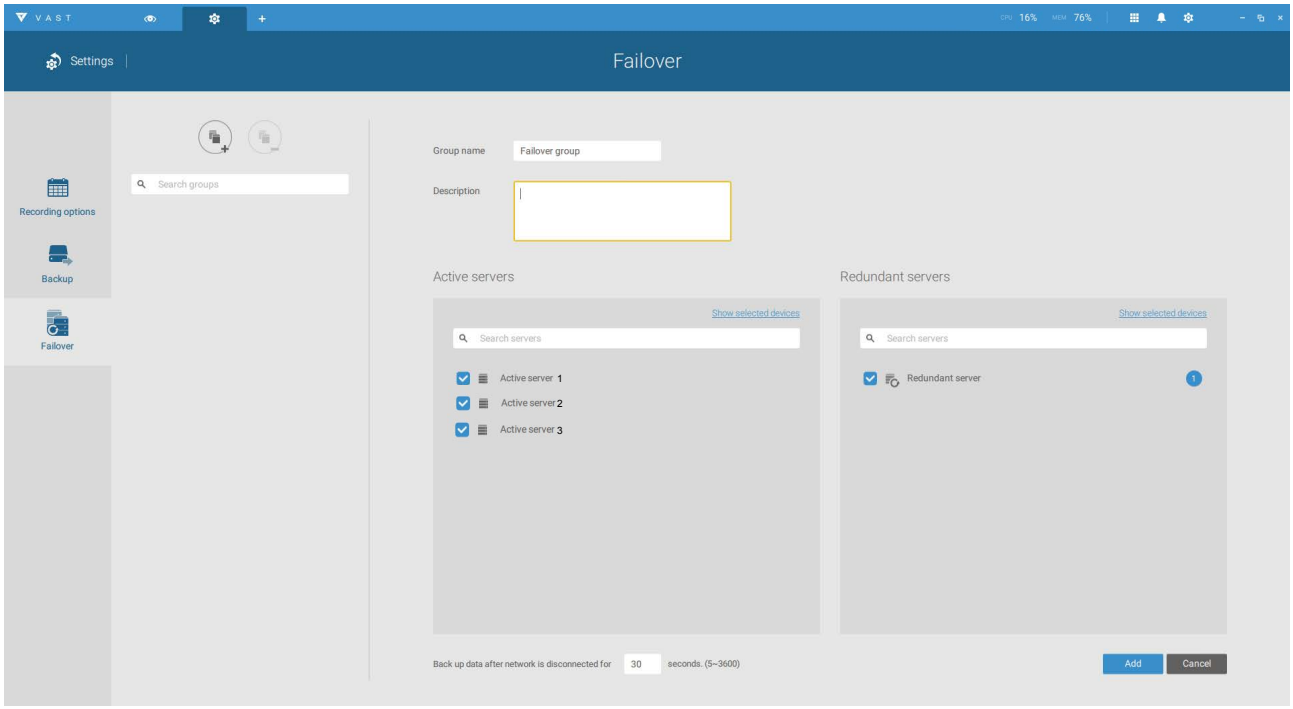
Two agents will be running on the Active and Redundant servers, "stunnel" and "VMSWebServer." Make sure they are not blocked out by your firewall. These agents can be found in the default folders below:

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



Click on the Add button 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.



3-3. VCA (Video Content Analysis)

The VCA Report utility is started from the tool bar on top,  . 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.

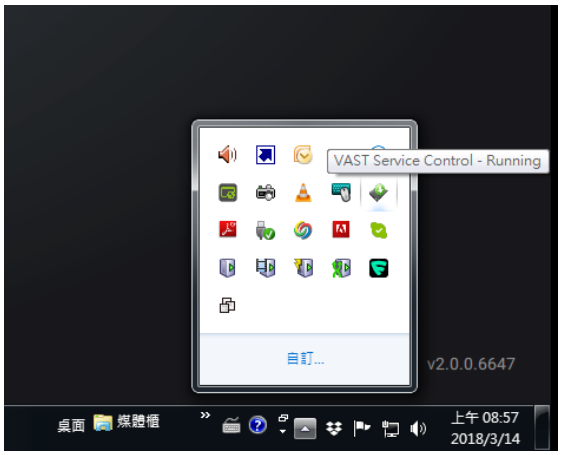
Note that the configuration of detection methods in People Counting still occur on a web console to individual cameras. It is not configurable through the VAST LiveClient.

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.



2. 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.

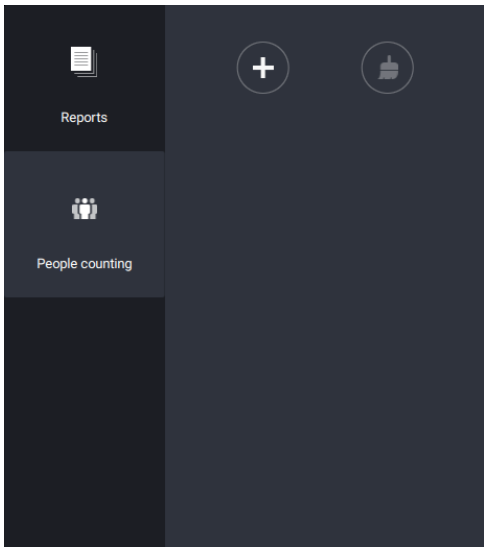
3. The life expectancy of VCA records is 5 years.

4. Currently the utility supports Windows XP, 7, 8, and 10.

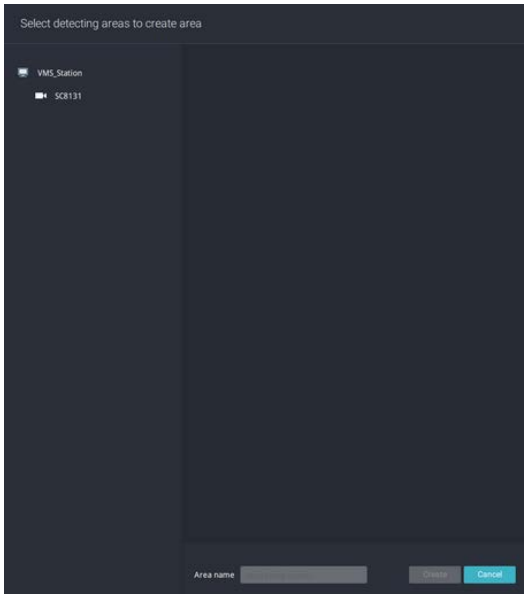
5. The latest revision VAST supports Seamless Recording, in order to retrieve collected data and recording during Ethernet disconnection. Provided that an SD card is installed on the VCA-enabled cameras, the VAST station gradually retrieves data from the SD card after the connection is restored.

To start VCA report:

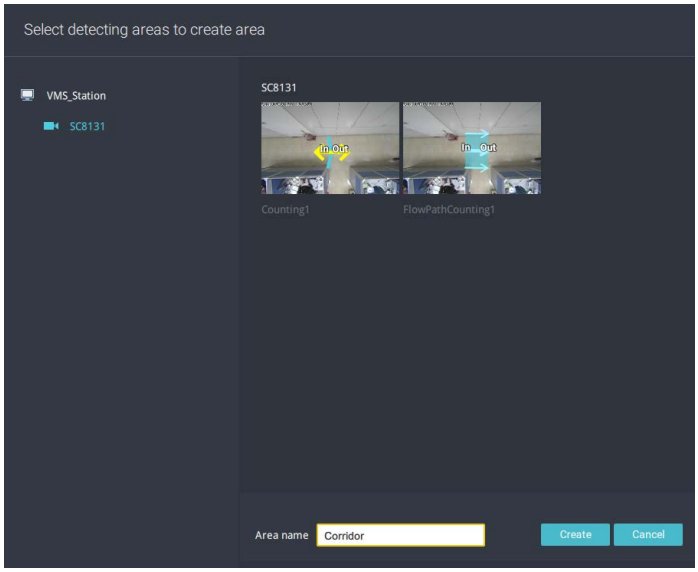
1. Click on VCA report button on the tool bar.
2. Select People Counting.
3. Click on the Add area button.



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

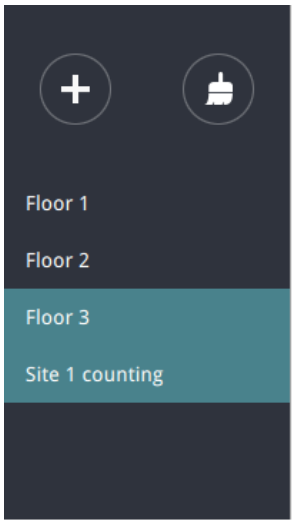


5. The pre-configured counting rules (areas) will automatically display. Select a counting rule and enter a name for the area. When done, click the Create button.



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

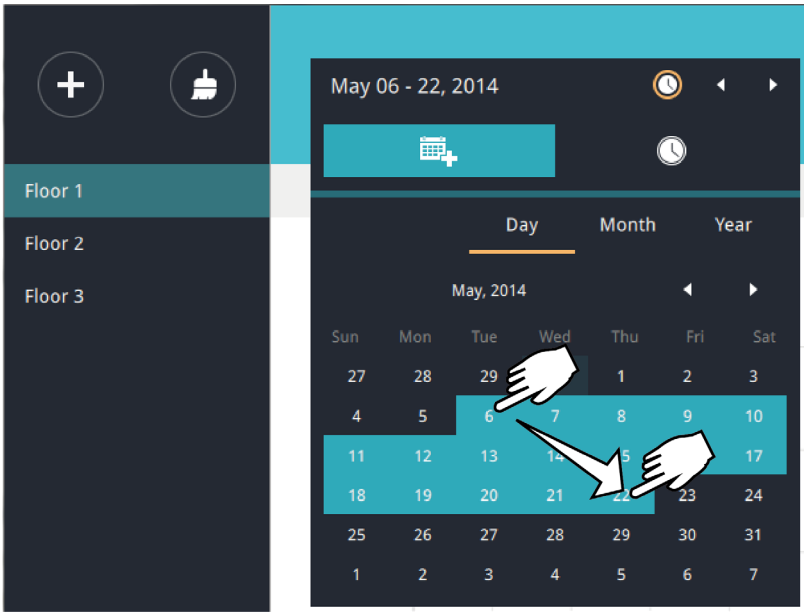
7-1. By default, the time displayed on the calendar is the current system time on the client computer running the utility. Select from the **Date** selector on top.

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.

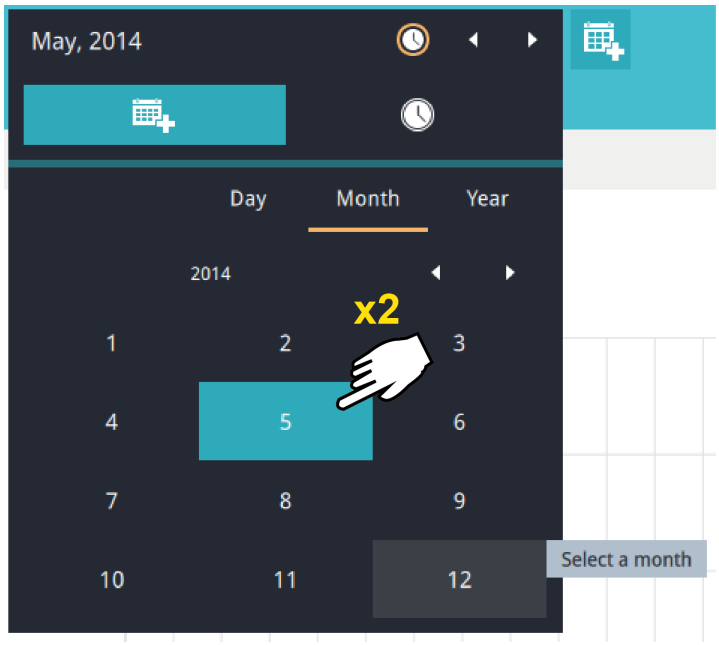
> You can select a month or a year using a single click. If you select a month, the timeline unit will be days within the month. If you select a year, the timeline units will be the months in a year.

> In the **Month** or **Year** panel, single click to select the entire month or an entire year. Double-click 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.

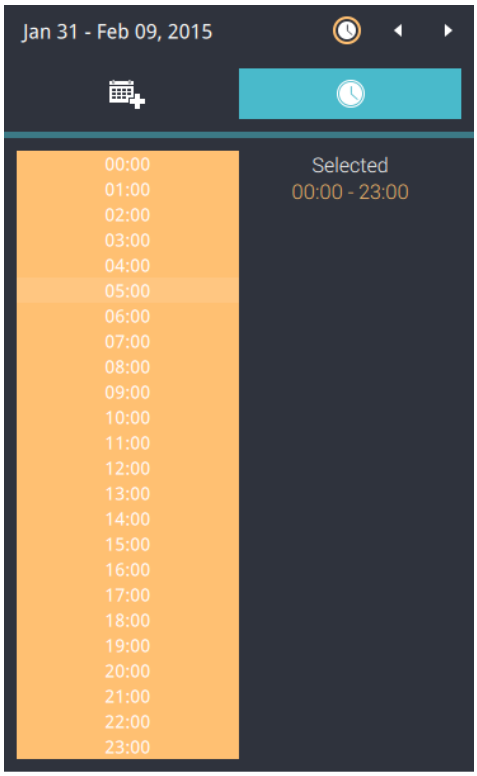


Note the following when making the configuration:

- 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.

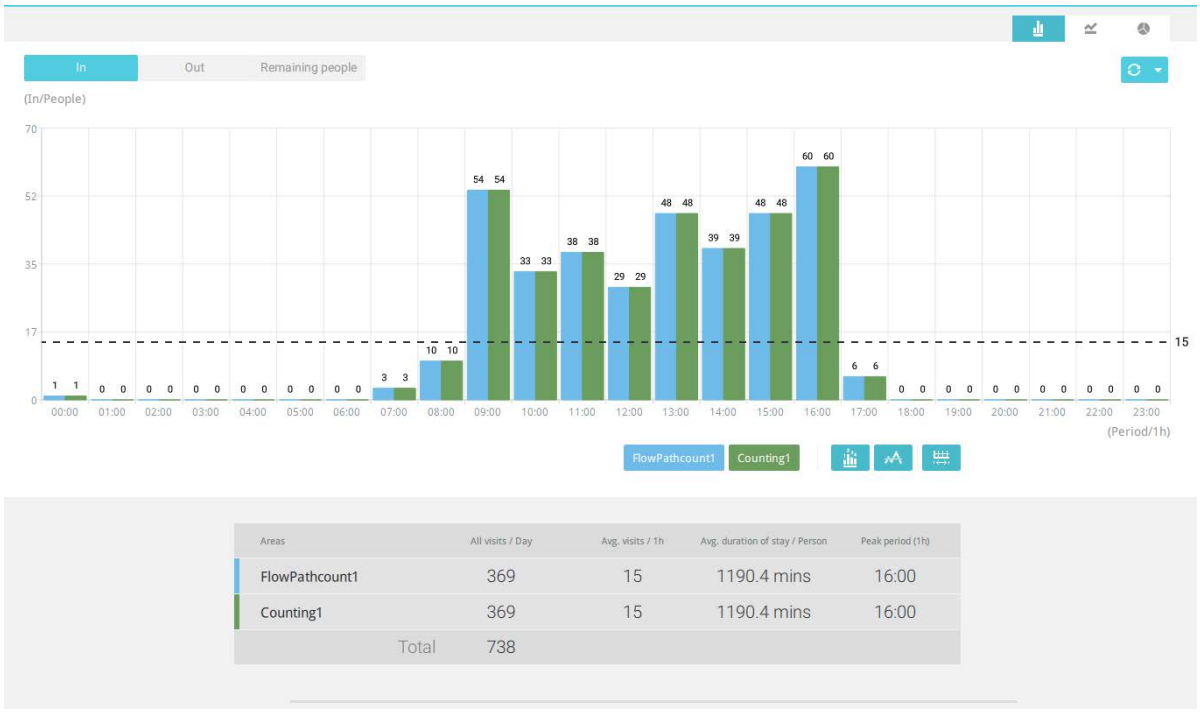
7-3. Select the hours to be included in the statistical poll using multiple clicks on the chart.

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



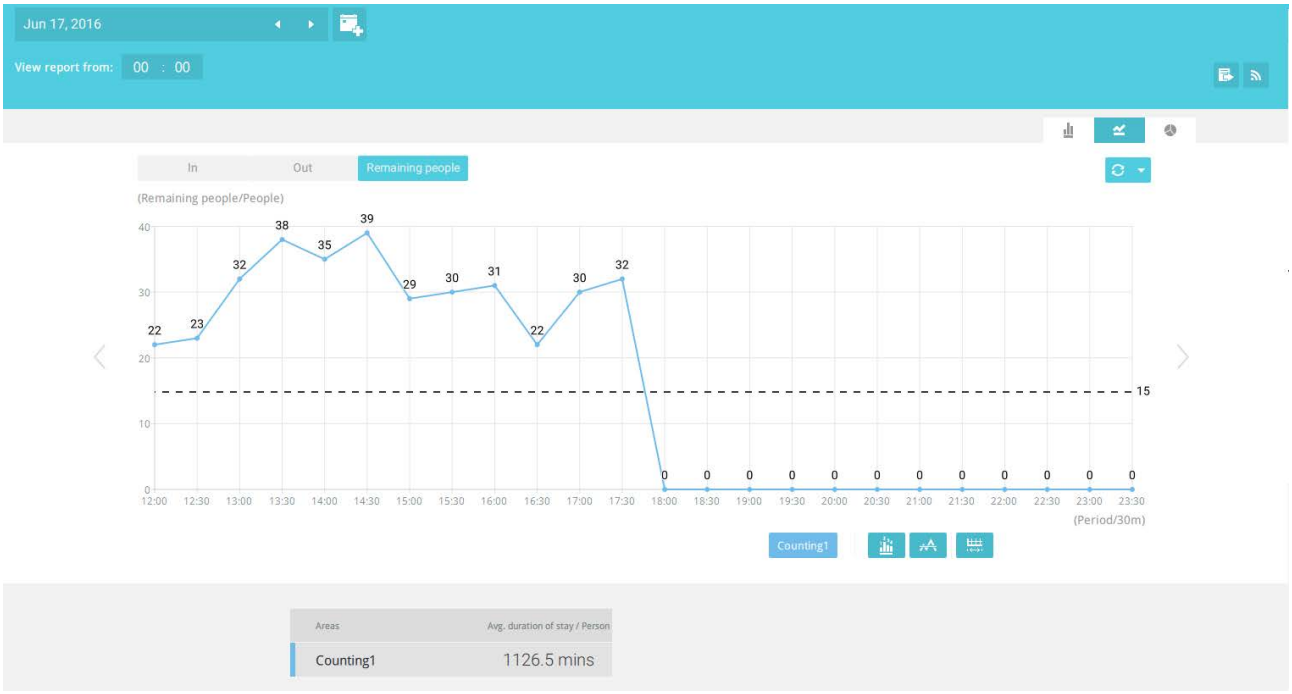
Note that you can only compare the counting results from two spans of time if you select only one Area. If you selected multiple Areas, you can not compare the results from multiple time spans.

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.



Areas	All visits / Day	Avg. visits / 1h	Avg. duration of stay / Person	Peak period (1h)
FlowPathcount1	369	15	1190.4 mins	16:00
Counting1	369	15	1190.4 mins	16:00
Total	738			

Select different display modes using the **Bar** , **Line** , or **Pie** chart buttons.



Areas	Avg. duration of stay / Person
Counting1	1126.5 mins

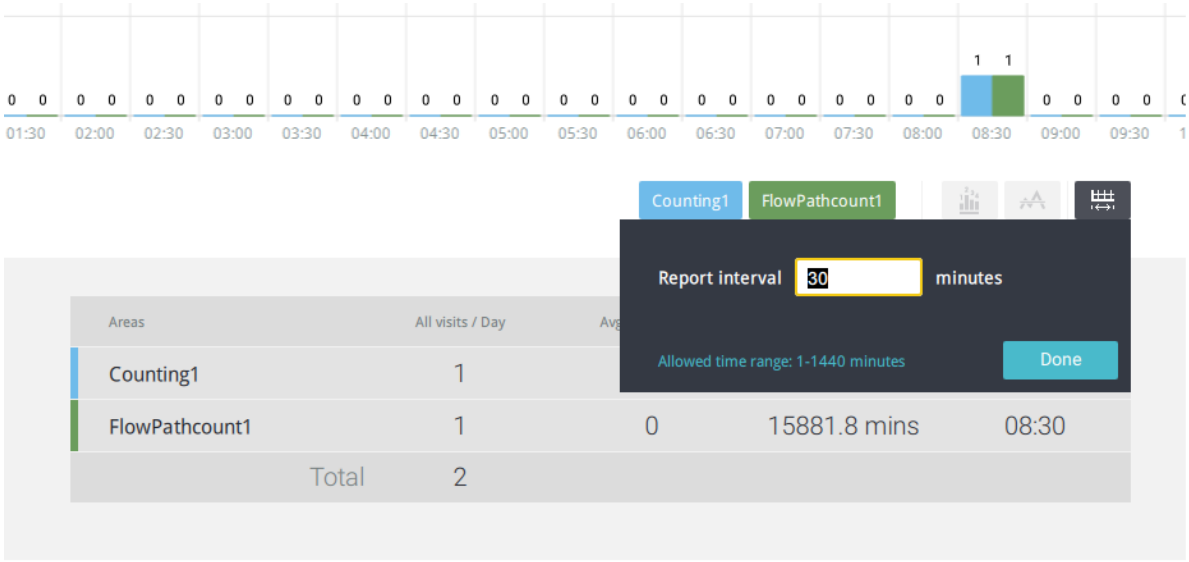
Note that the timeline units can vary depending on the span of time you selected on the Calendar panel. If a date was selected, hourly data will display in chart. If a year was selected, monthly data will display in chart.

Use the following functional buttons to change the display parameters

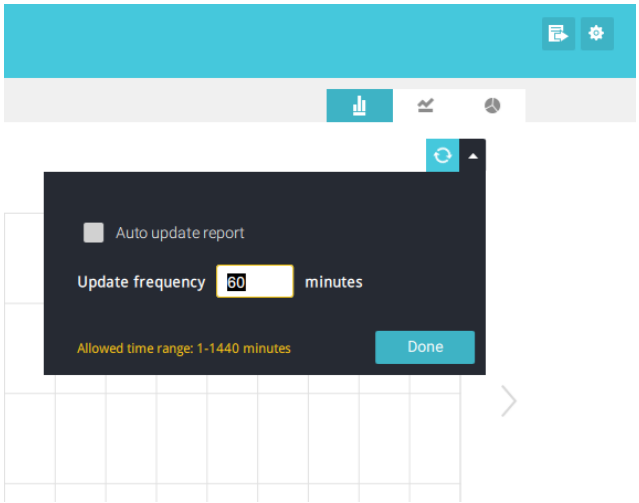
Show data on chart : Displays the collected numbers on chart.

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.



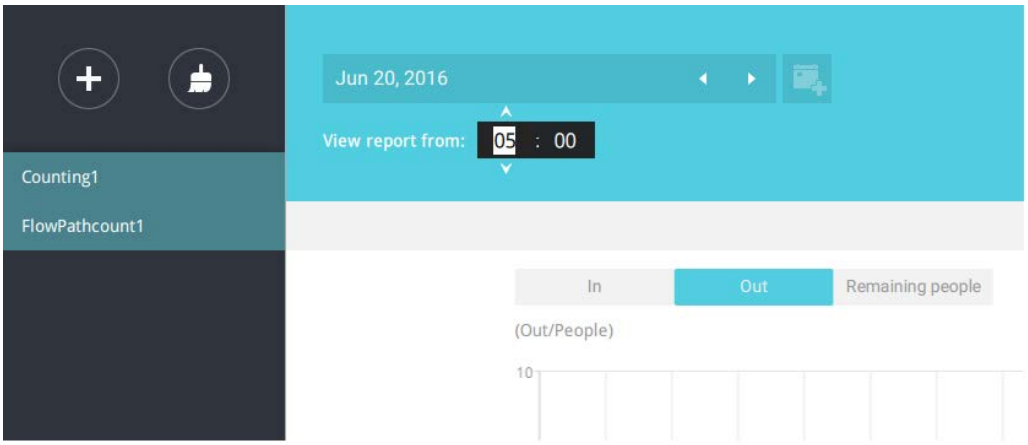
You can use the update menu on the side of the Refresh button to determine an automatic update schedule. You can let the statistic chart update itself by a regular interval.



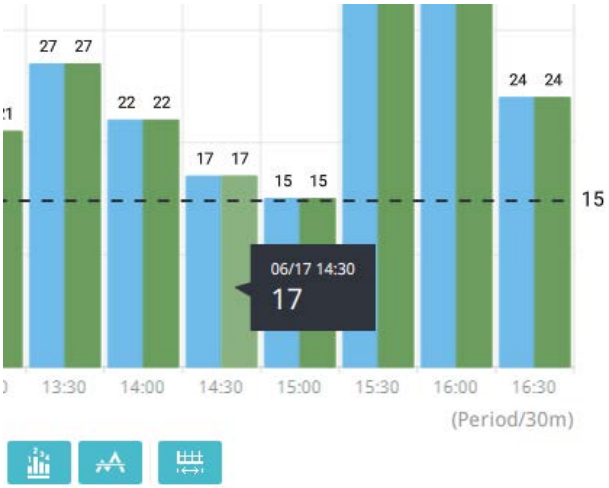
If you selected only one area, you can use the Shift key to select multiple areas (or two spans of time). You can select multiple dates in the Calendar panel.

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

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.

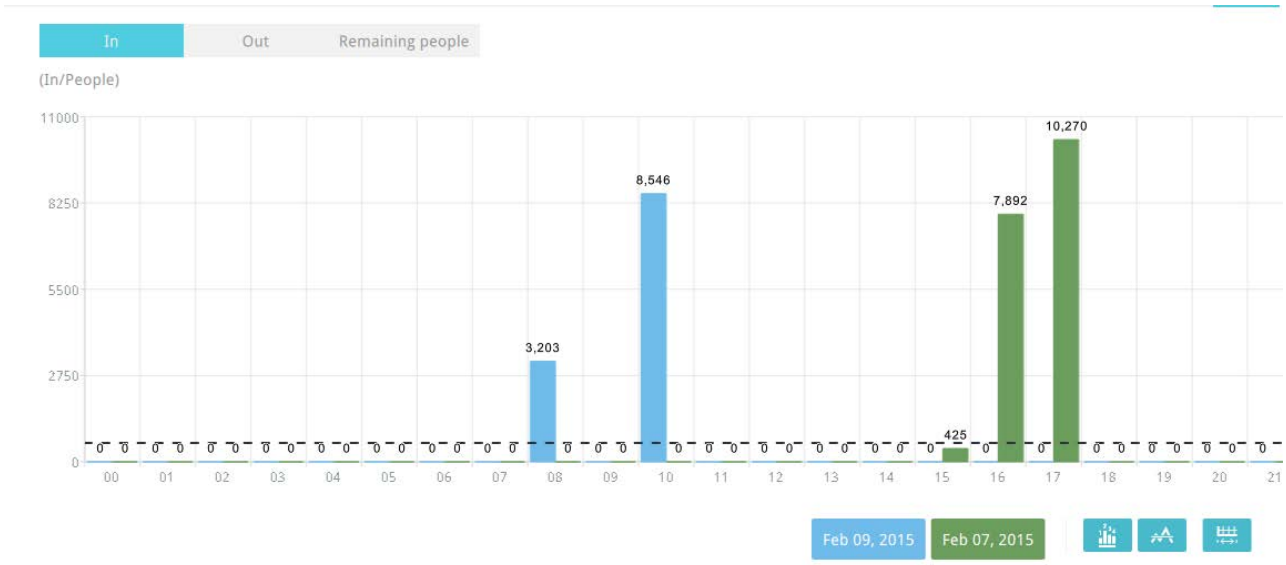


A number is displayed when you mouse over an area on the chart. Move your cursor to an area on chart, and the number is displayed.

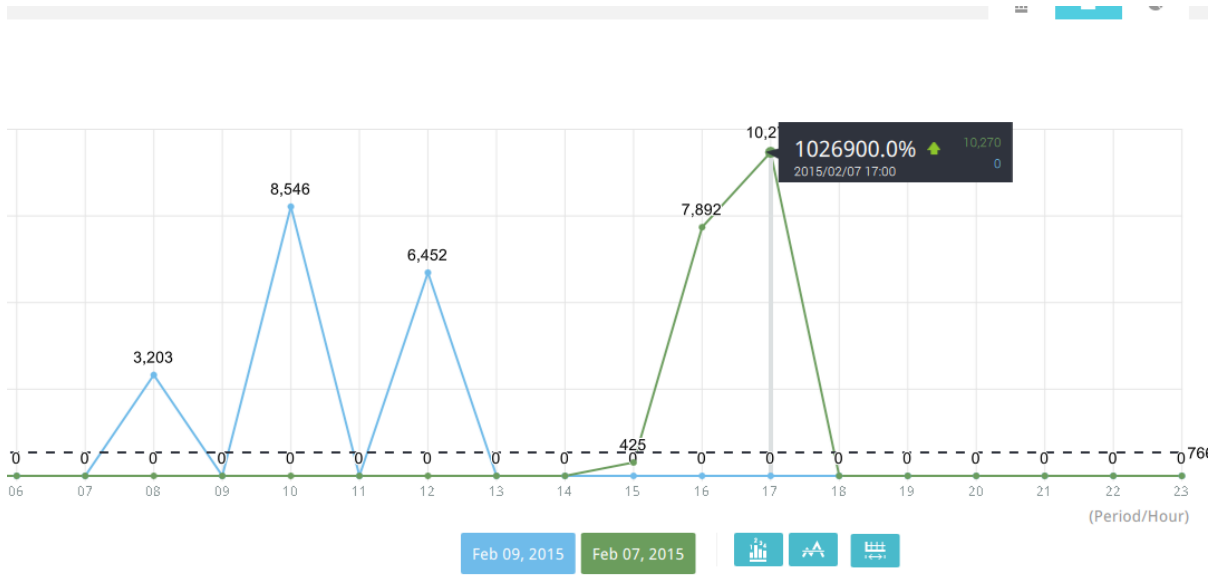


Data on a time line will be generated. To close the window, use the close button on the second date information. Equivalent spans of time can also be used for comparison. For example, you can compare the data in a span of 4 days against another span of 4 days.

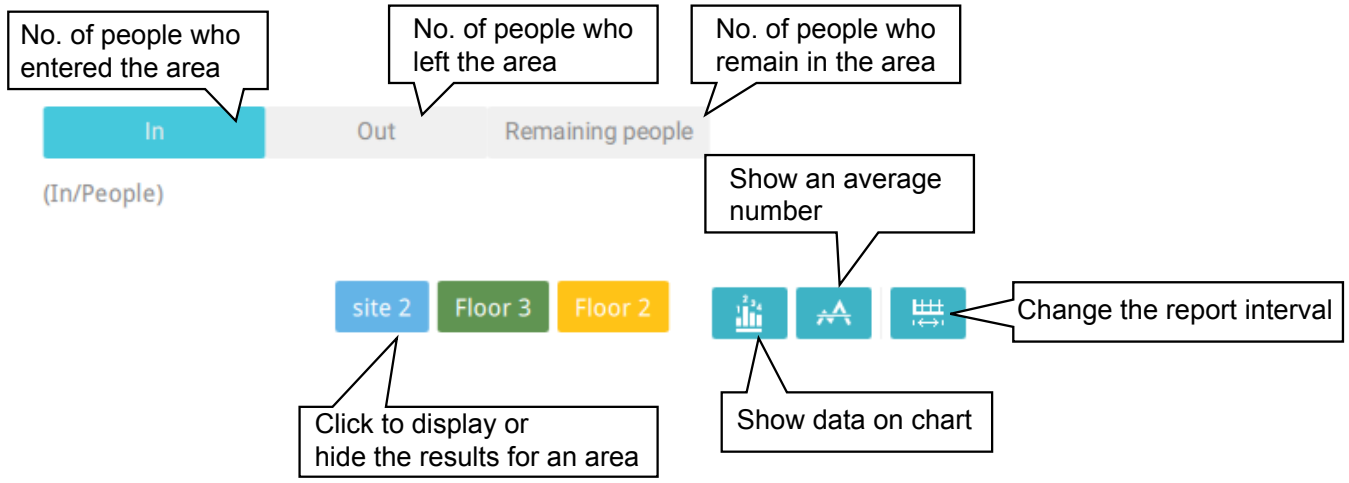
Note that the Compare function only applies when you select to display only one area on screen.



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.



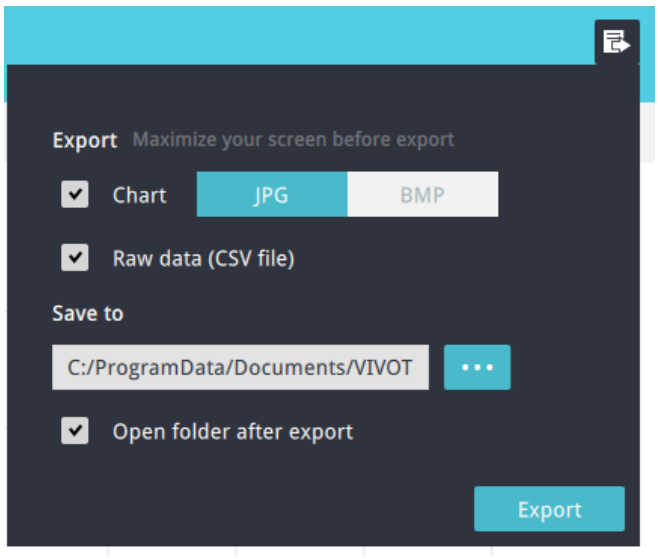
See below for the functions of buttons on screen.



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

9. 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.

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.

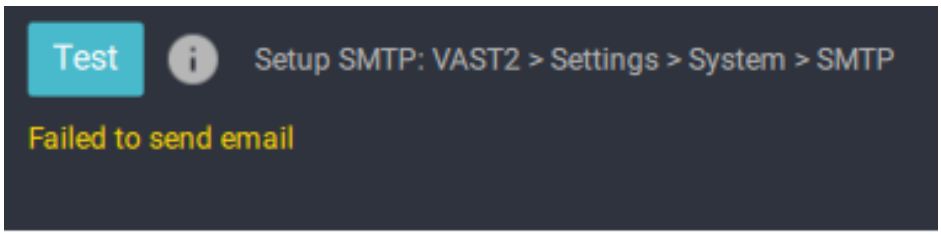
Note that the notification contents is your current field of view, including a Bar, Line, and Pie chart combined into one image file. The In/Out/Remaining results will be generated into 3 charts. Each Area will generate one CSV file, and each CSV data file will contain In/Out/Remaining/Summary information.

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).

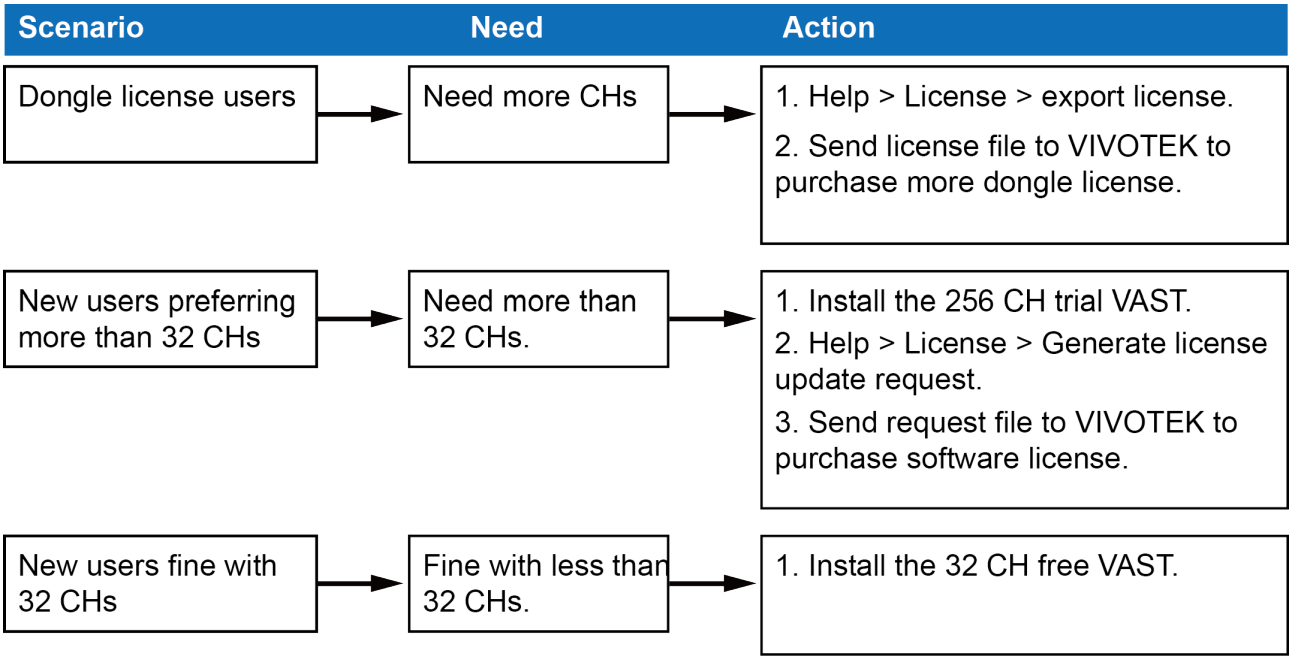
You may configure to receive regular VCA report as Weekly or Monthly using the associated menus.

Below are the messages with the Email test function.



3-4. VAST Software License

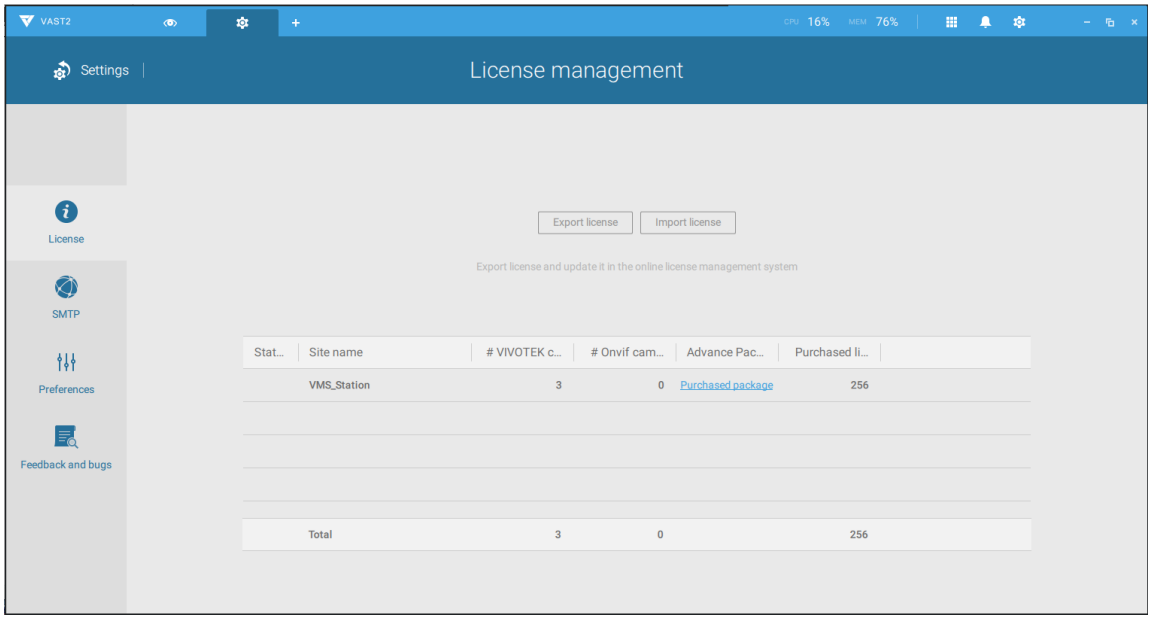
To activate the software, refer to the flow chart below:



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 **Help** > **License** page, and click on the **Export License** button. Send the request back to VIVOTEK to purchase more channel licenses.



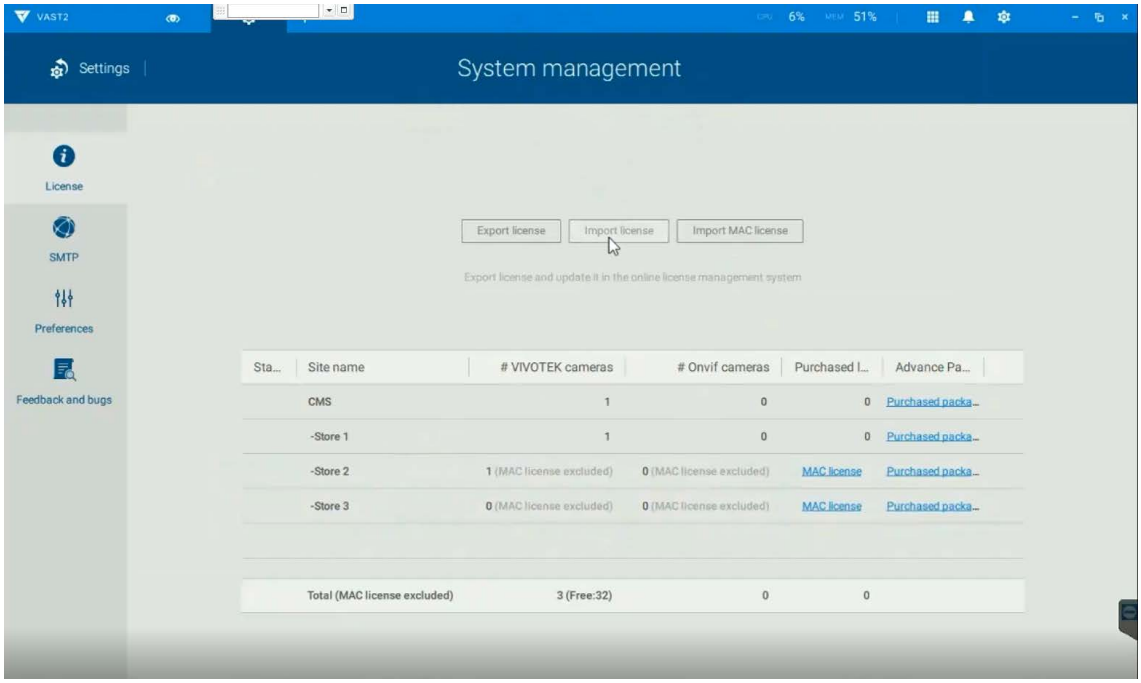
When you purchased and received the official software license, use the **Import License** function to activate the official license.

When importing purchased licenses, you can manally select which station/license file to update, or click the **Auto Dispatch** button and let system decide the distribution of license updates especially when there are substations under a managing VAST server.

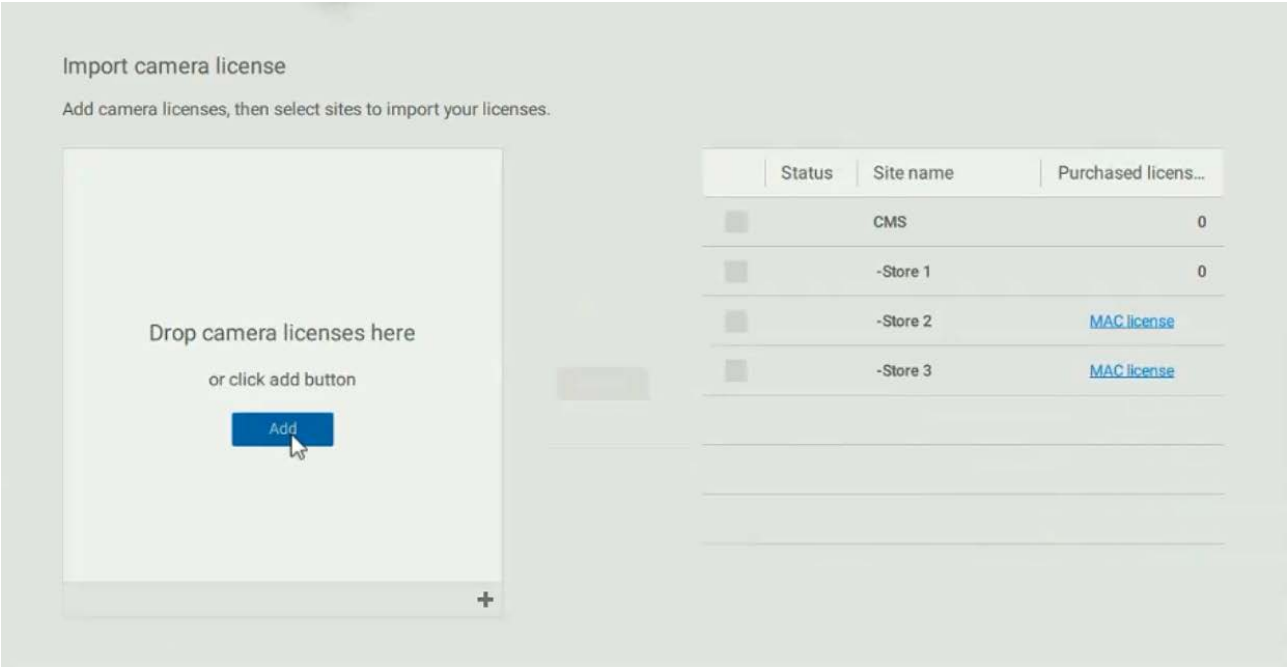
Before the Auto Dispatch function is available, license has to be individually updated on every substations.

Below is a sample procedure for importing the camera licenses:

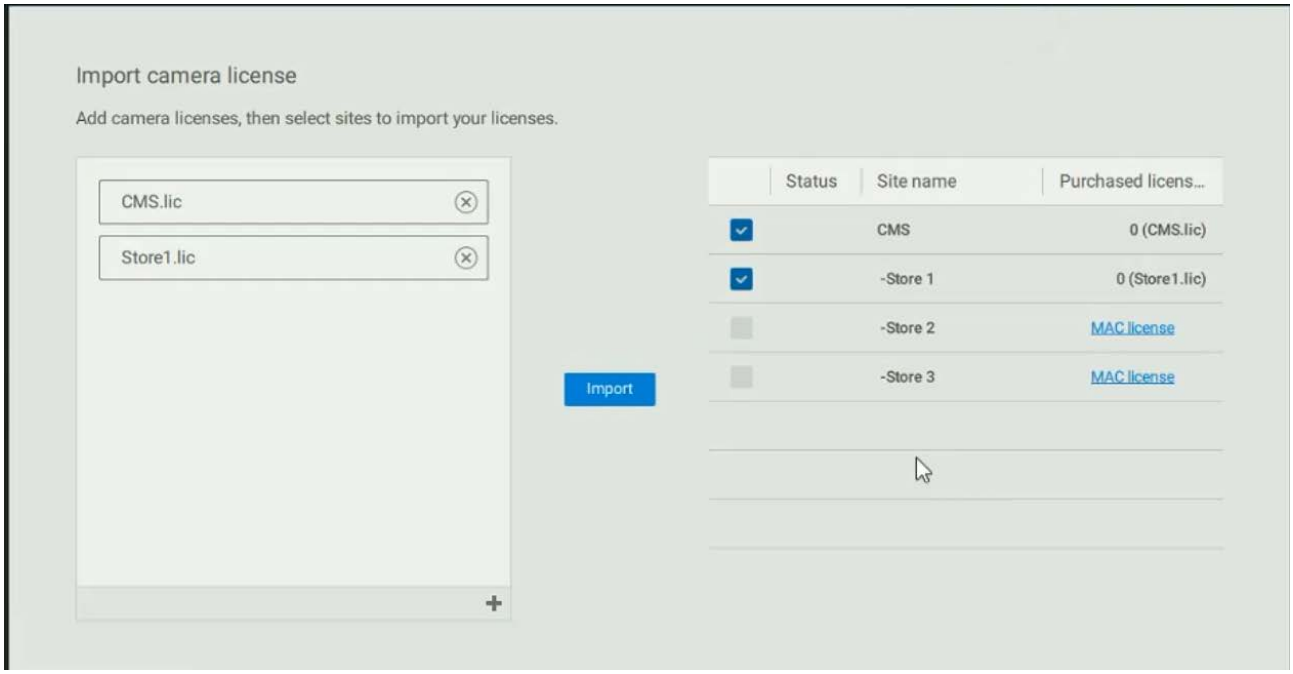
1. Continue to import the camera licenses.



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

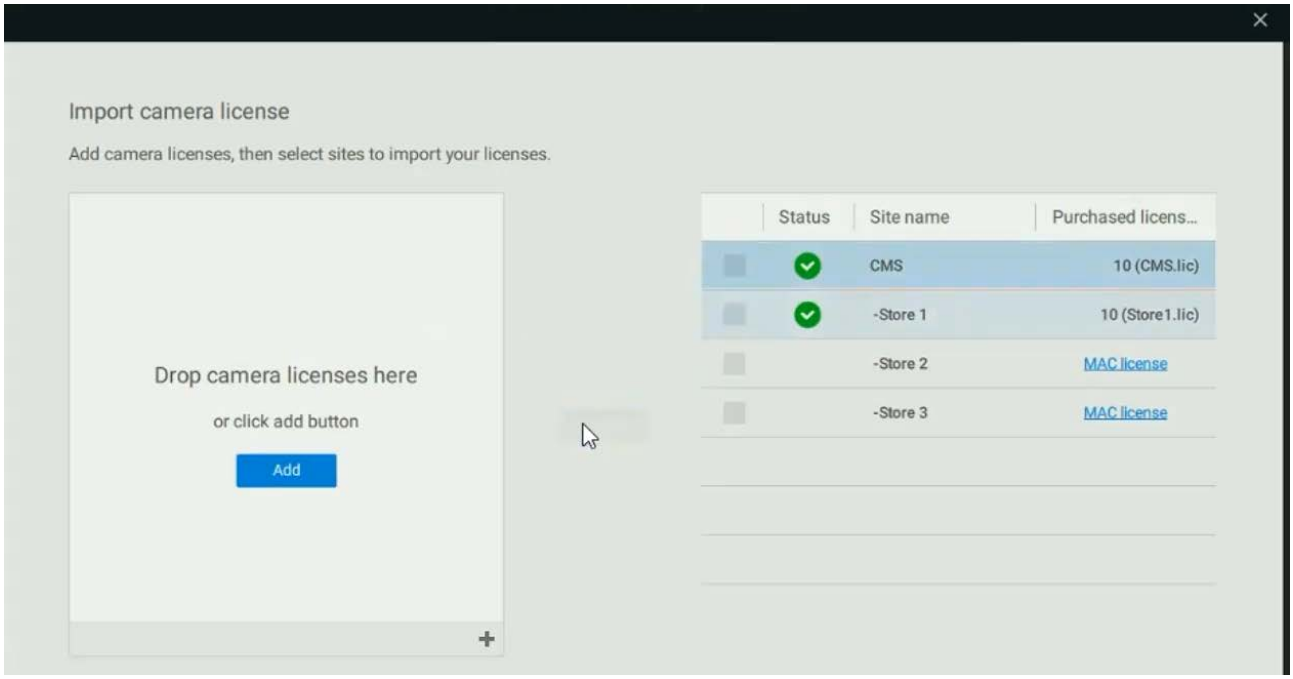


3. Select the target servers, click Import.

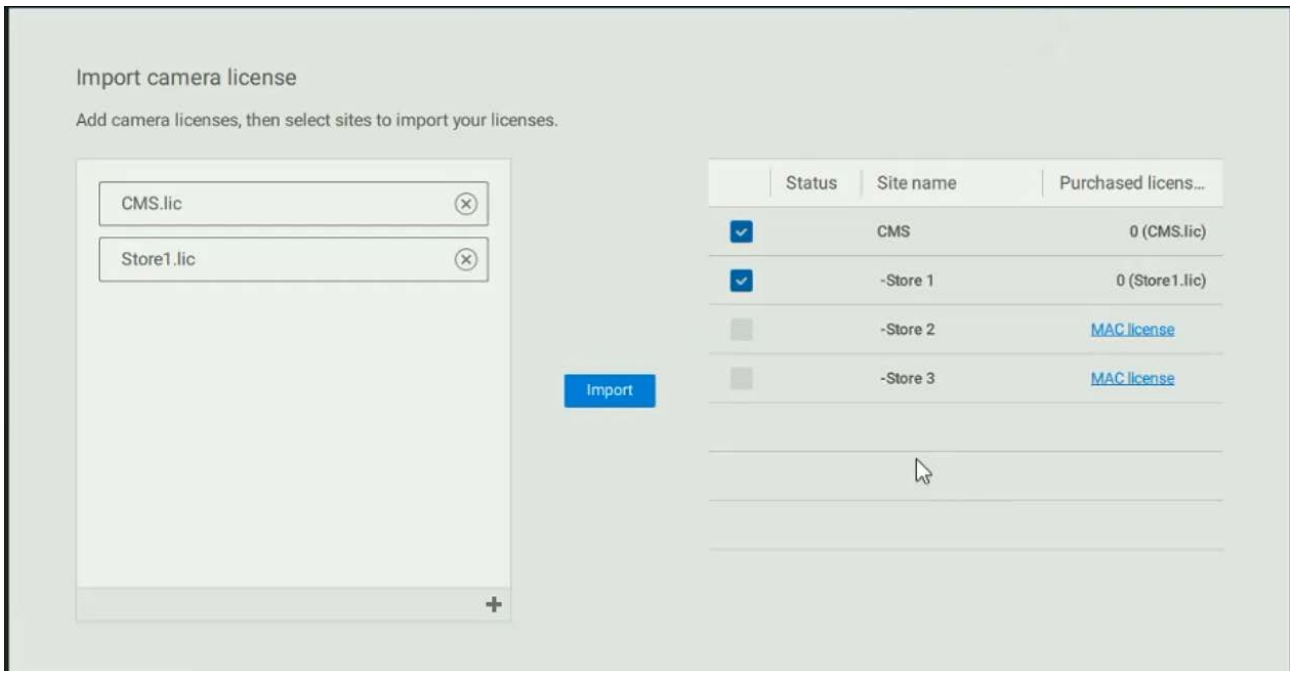


4. When done, a successful import will be indicated.

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



5. Select the target servers, click Import.



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. It does not work if it is generated from a VAST2 installed on a non-Virtual Machine.

This instruction includes:

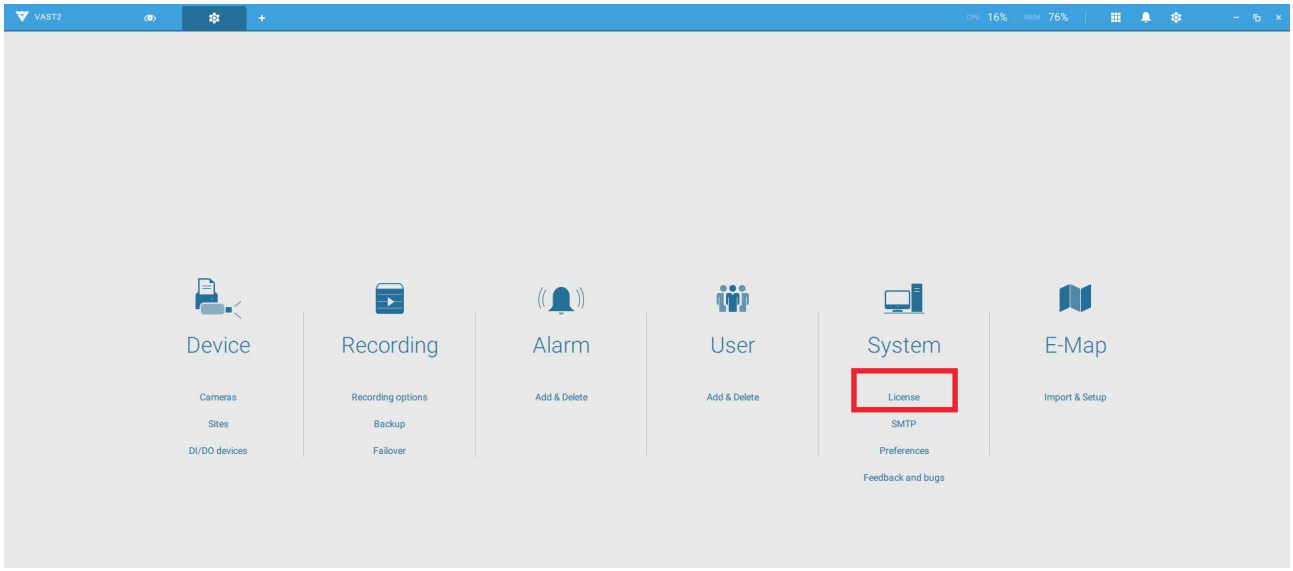
1.How to Export a license request from VAST2 on a virtual machine.
2.How to acquire the MAC addresses of the inserted or non-inserted cameras?
3.Send us request files & MAC addresses (If you have multiple sites, please remember to designate grouping information, such as which MAC addresses belong to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

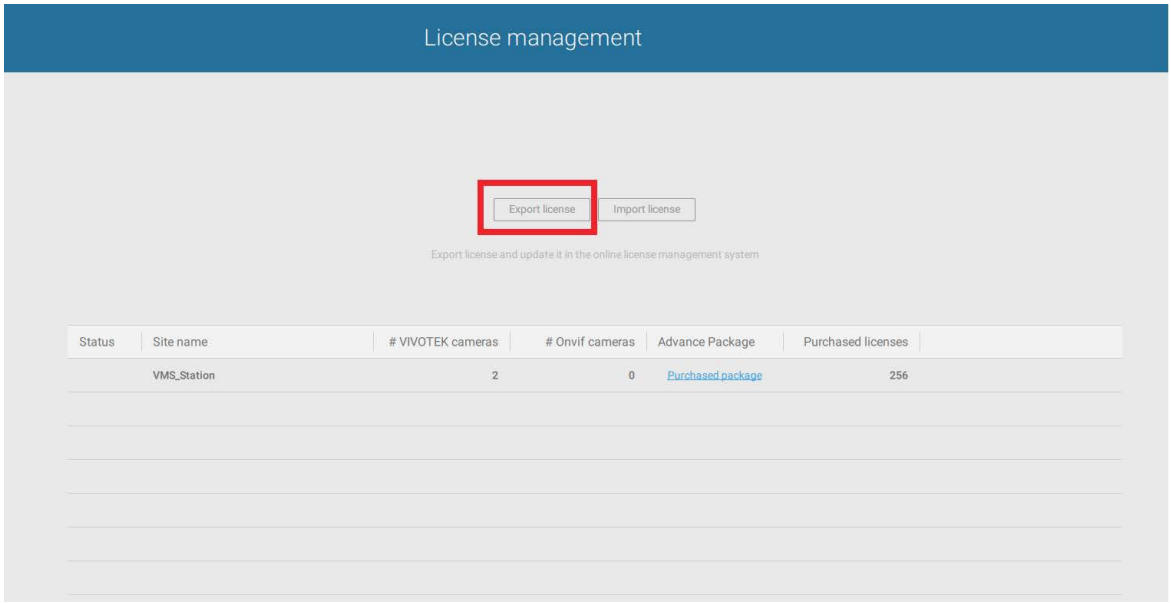
1.How to export request from VAST2 on VM?

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.

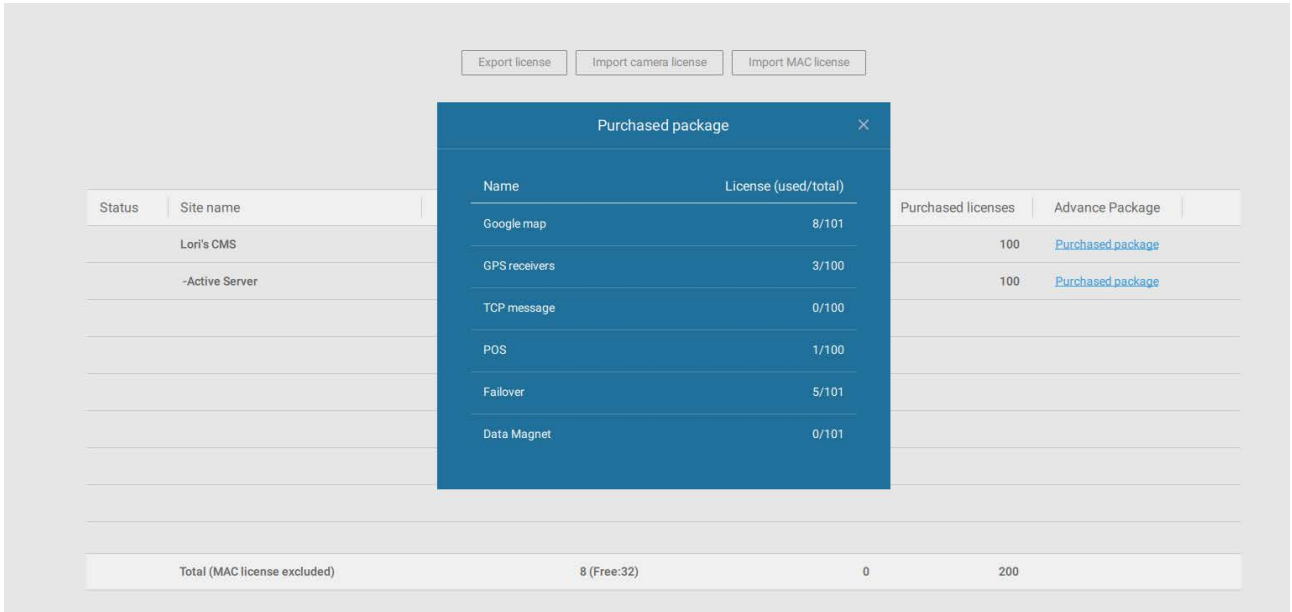




1-4. Click the Export license button and select your Windows desktop as the destination folder. A VAST2 license folder will display on the desktop, zip the folder and send the request file back to your sales representative, distributor, or VIVOTEK.

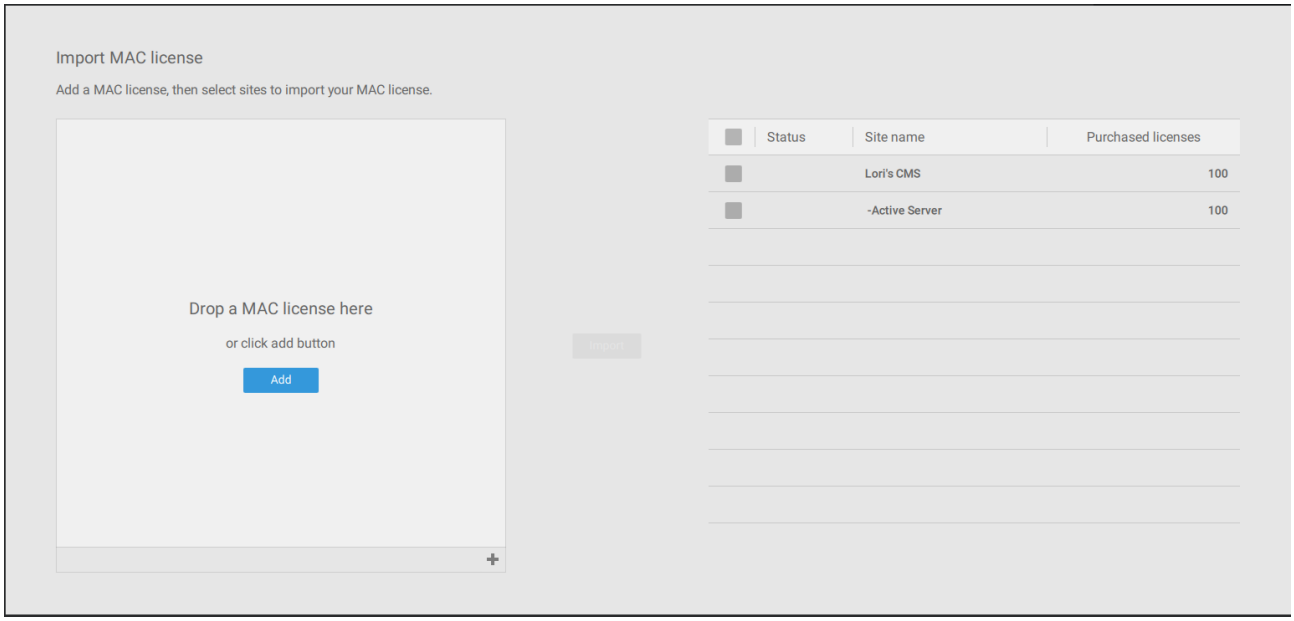
The generated MAC list should look like this.

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

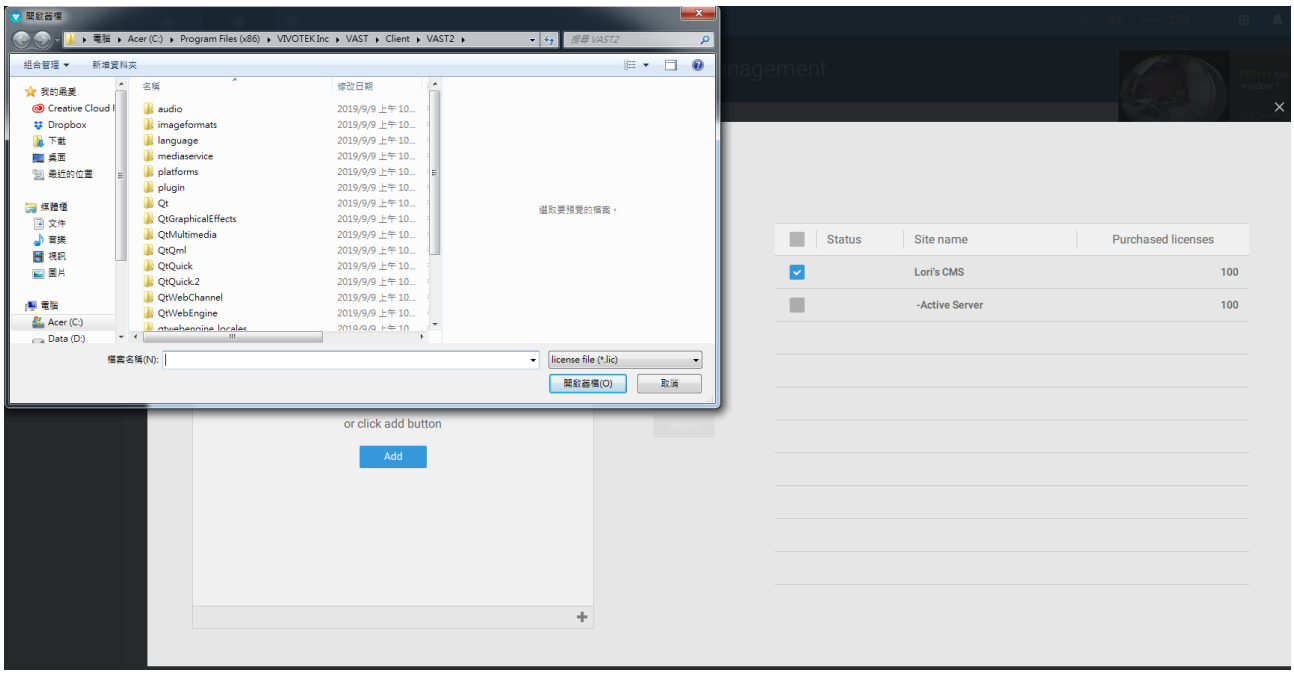


1-5. Once you acquired the MAC licenses from VIVOTEK, click Import MAC license button. You will enter the import page. Use the Add button and locate your license files.

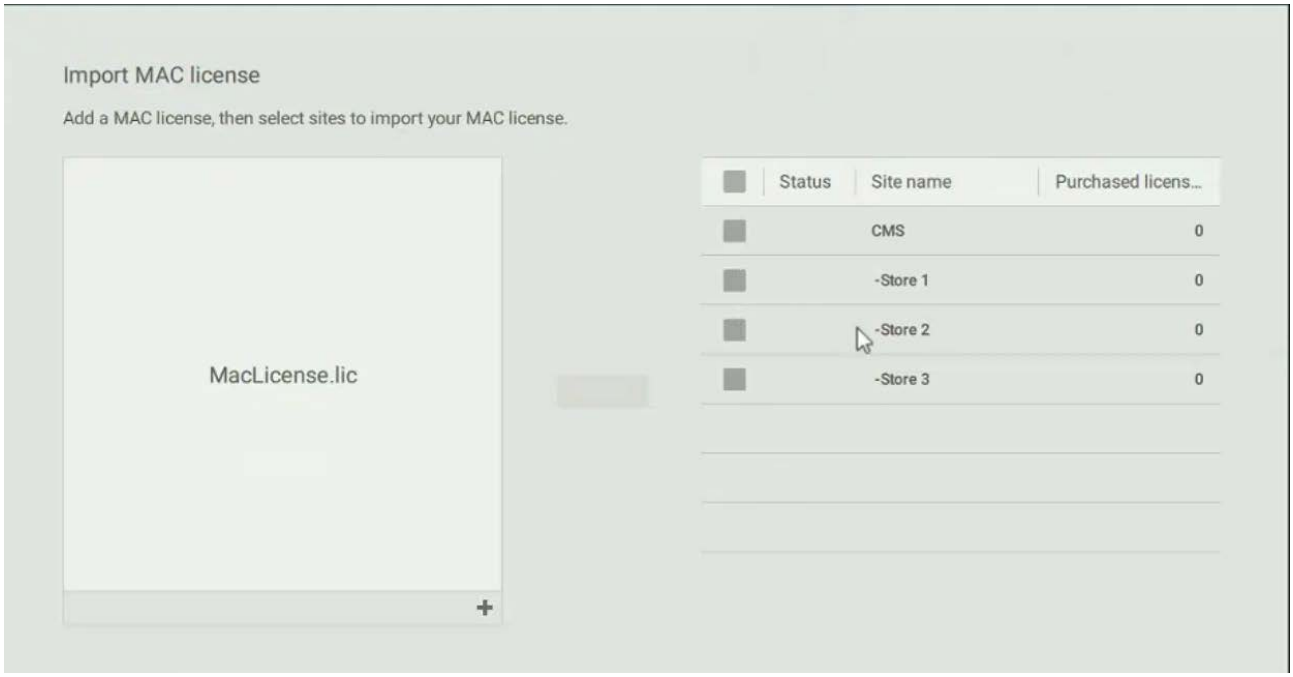
To use the MAC license import function, both the CMS and its substation servers should both be running VAST revision 2.6 or above.



1-6. Select the license file.

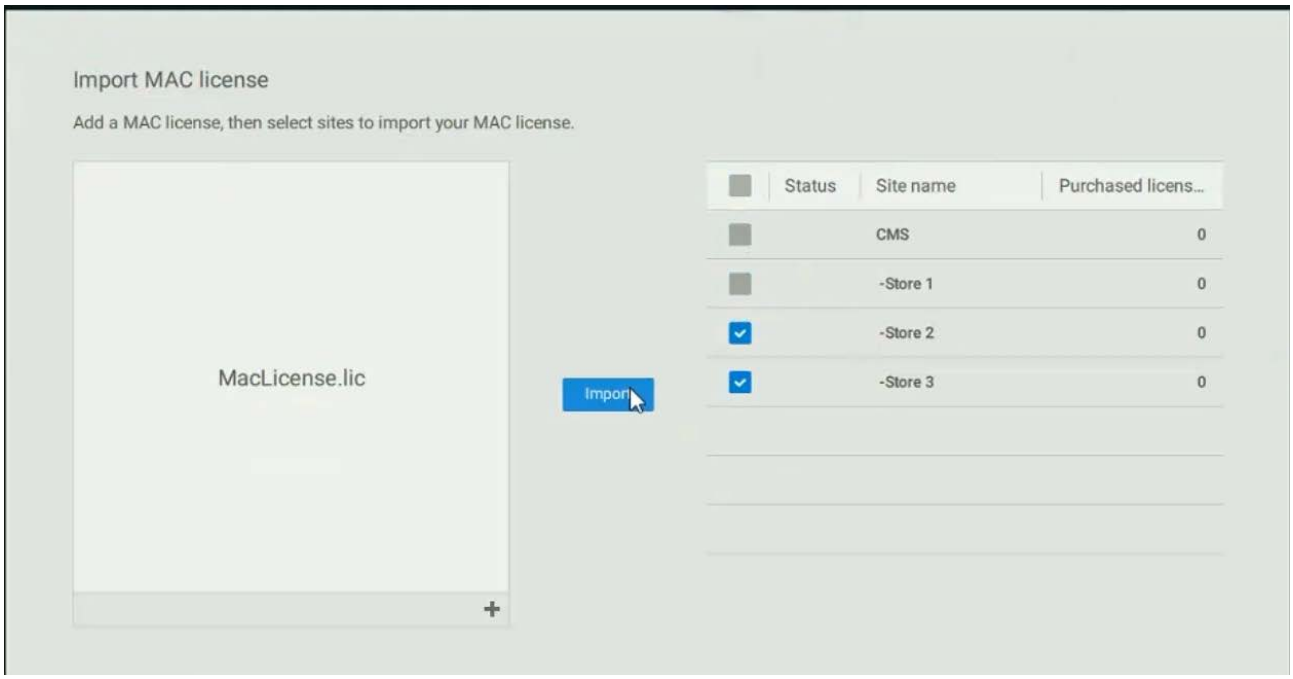


1-7. The selected file appears on screen.

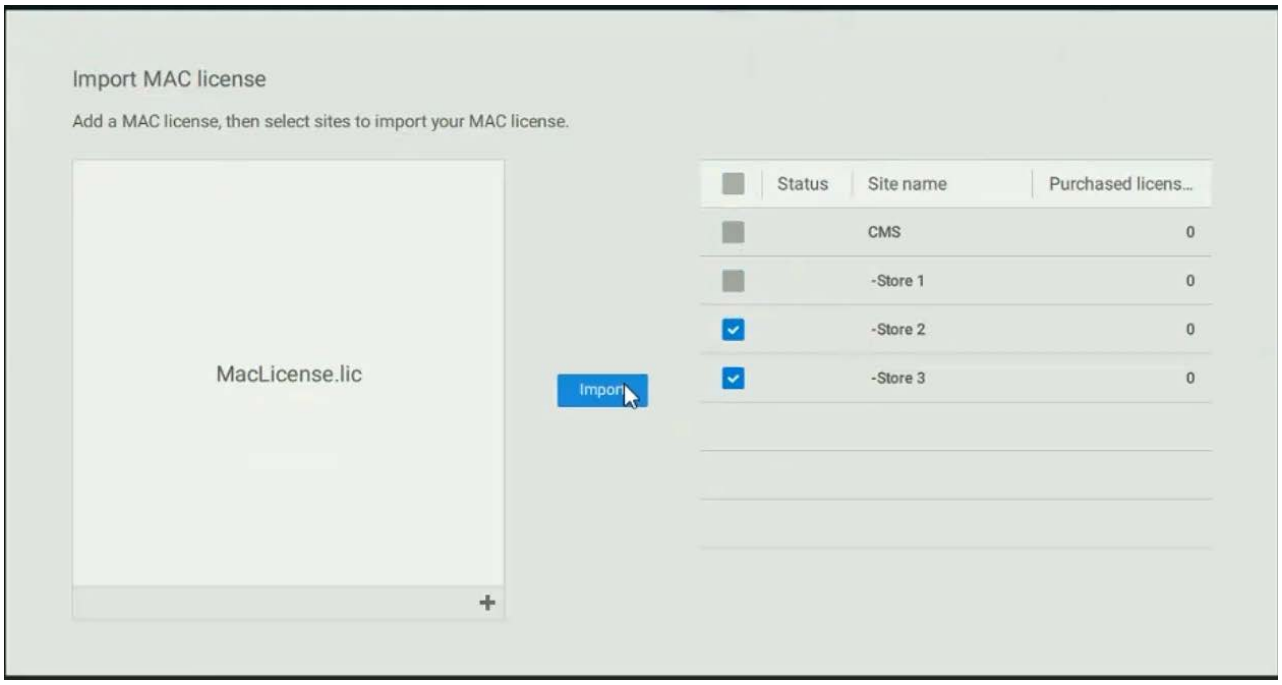


1-8. Select the target server sites to import the license file. When done, click the Import button.

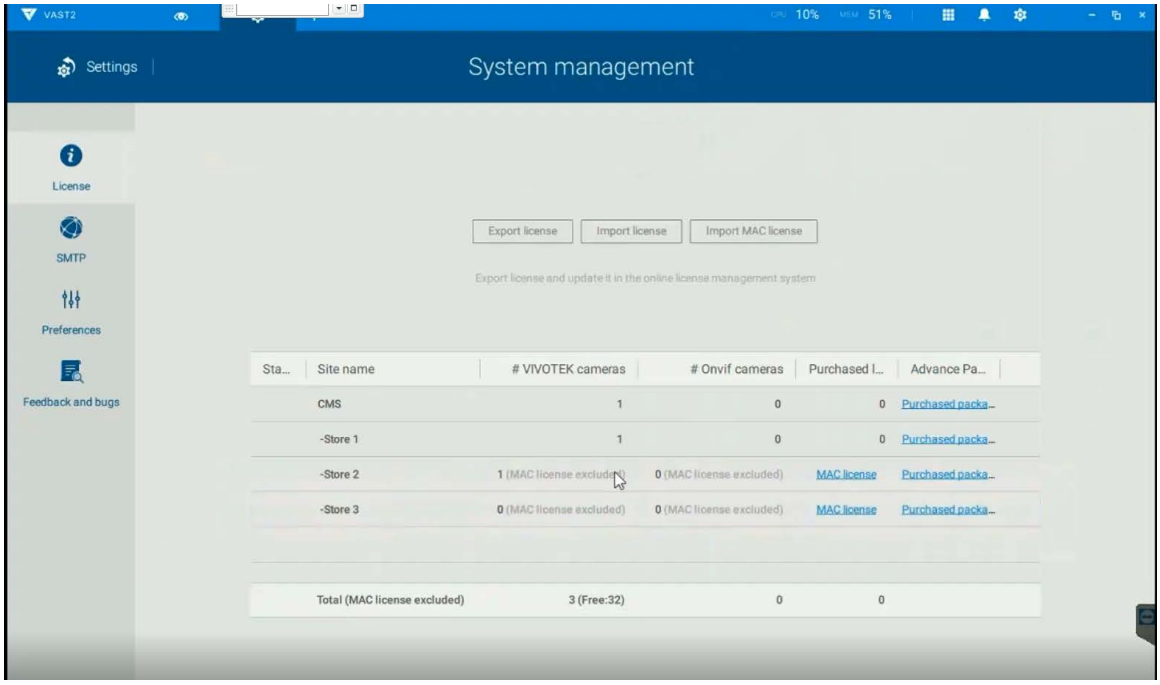
MAC licenses are not bundled with server hardware. You can import licenses from the CMS server to one or multiple virtual machines running the VAST software.



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



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

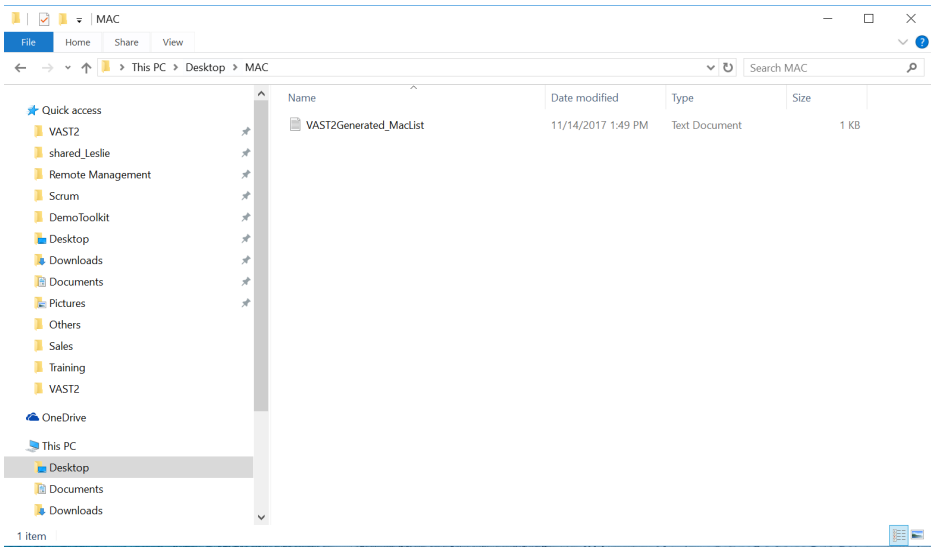


2.How to Acquire the MAC Addresses of the Inserted and the Non-inserted Cameras?

2-1. Search for the MAC addresses of the inserted cameras:

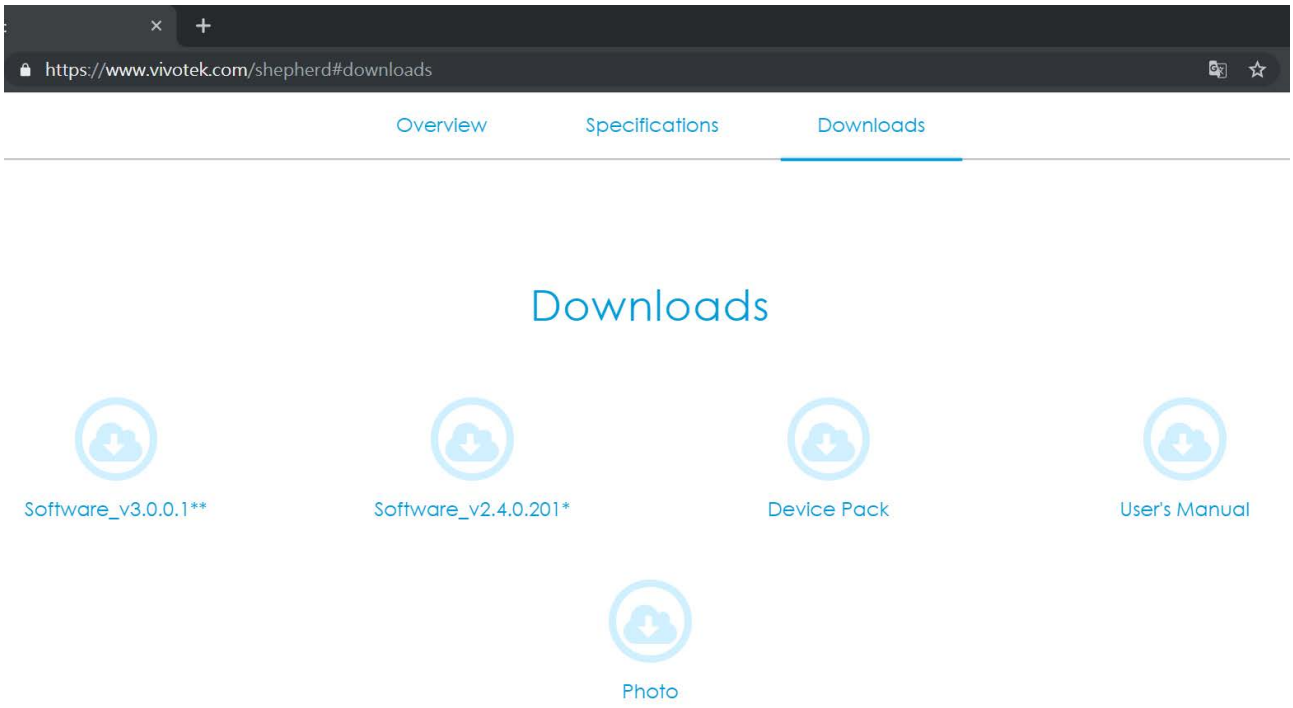
On the Settings > License page, press the Hotkey combination: **Ctrl + Shift + Alt + M**.

2-2. Open the Download folder and send us the file (VAST2Generated_MACList.txt). The MAC address related information is included inside.



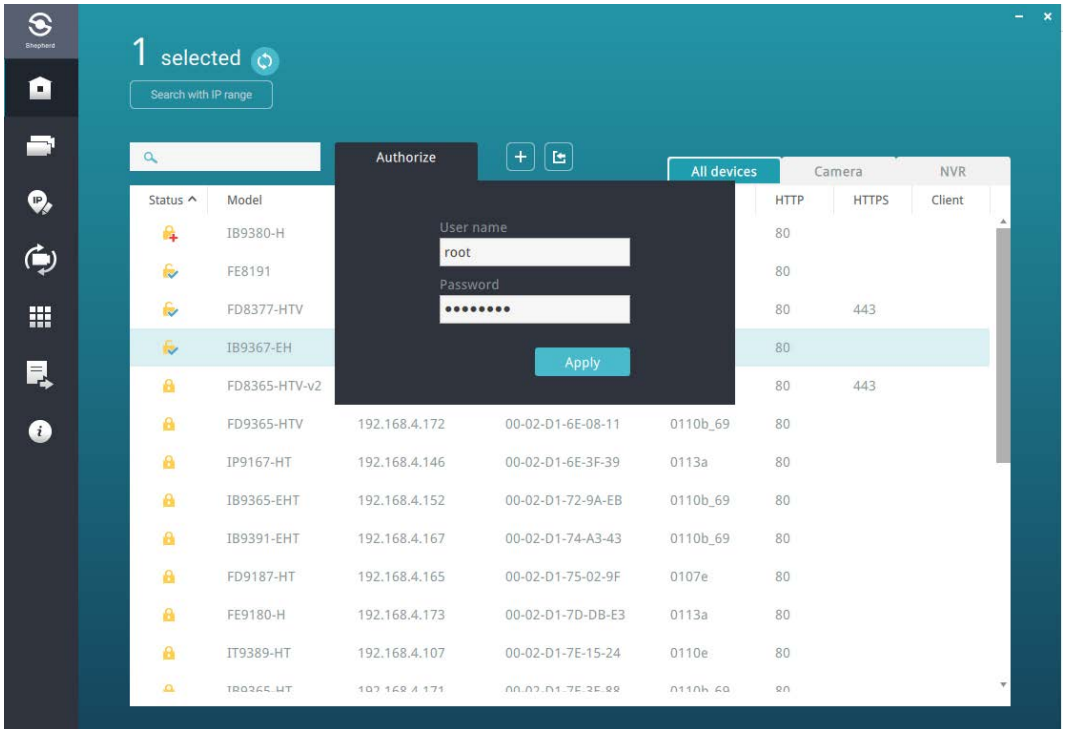
2-3. To acquire the MAC information of the cameras that have not been deployed using the VAST2, use the Shepherd utility.

2-3-1. Download the Shepherd utility from VIVOTEK website.

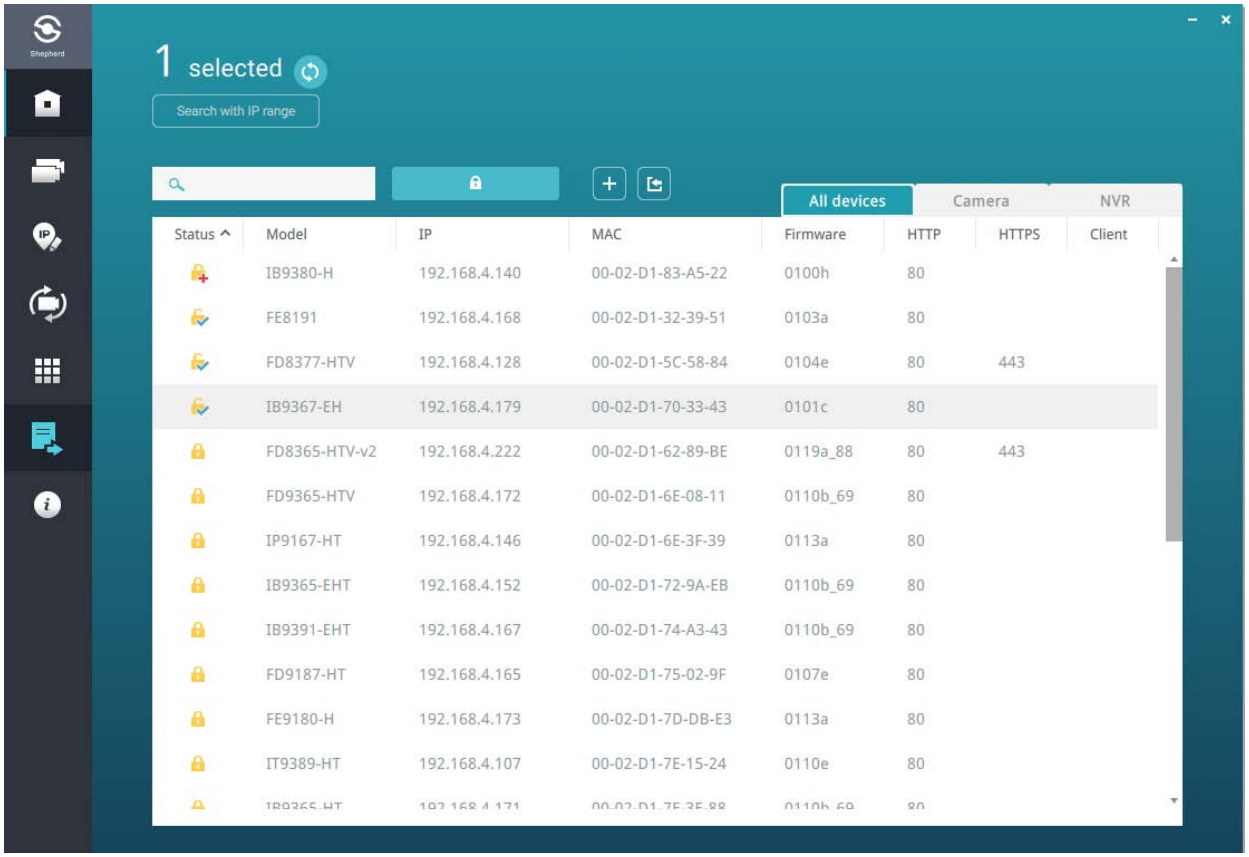


2-3-2. Double-click on the Shepherd.exe to run the program. It will search and list the searched cameras on LAN.

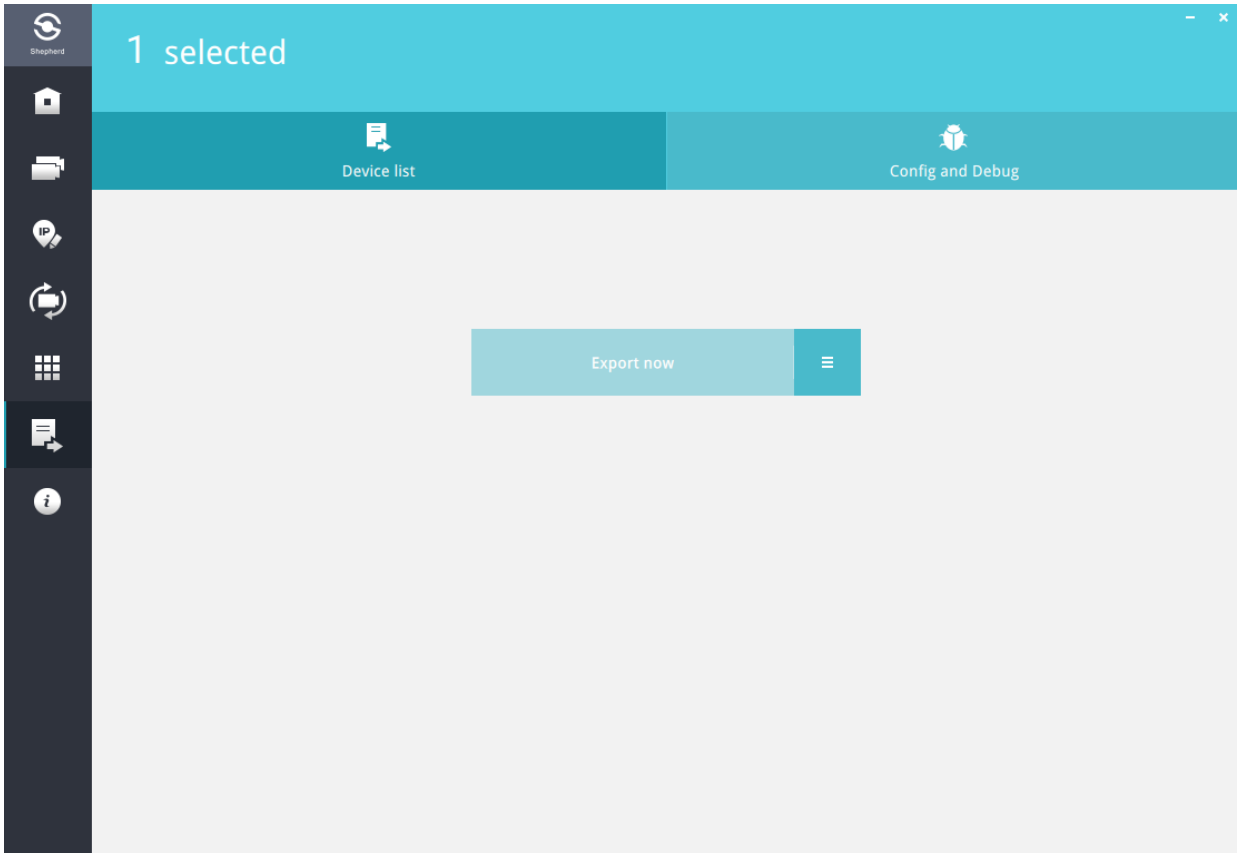
2-3-3. Authorize those cameras and select the cameras you want to enable their use in VAST2 by imposing a license.



2-3-4. Make sure the selected cameras have been successfully authorized, click on the “Export device list and debug report” button. Multipe camera entries can be simultaneously selected.



2-3-5. Click the Export now button.

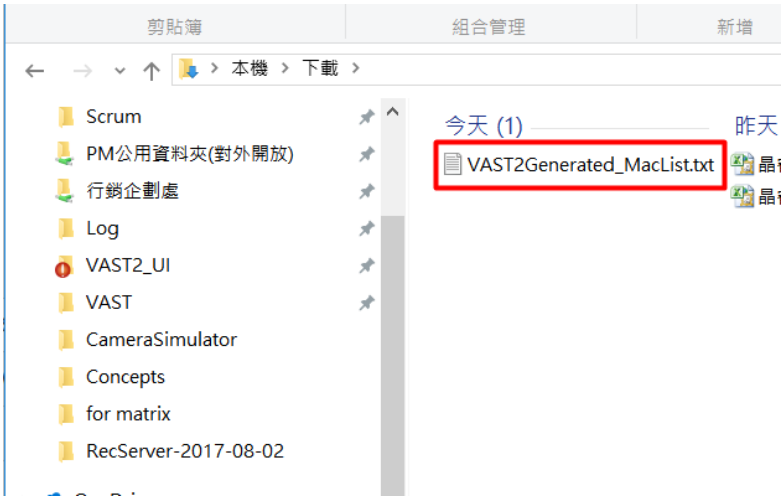


2-3-6. The exported contents will be stored as a csv file with the MAC information. Please send this csv file back to your sales representative, distributor, or VIVOTEK.

3. Send the Following Request Files & MAC Addresses to VIVOTEK

3-1. Generate the request file from a VAST running on a virtual machine. If the request is not generated from a VAST instance on a virtual machine, then an error will occur while updating the MAC licenses.

3-2. Send the MAC addresses of the cameras you want to insert. The file names should look like: VAST2Generated_MACList.txt, or shepherd csv.



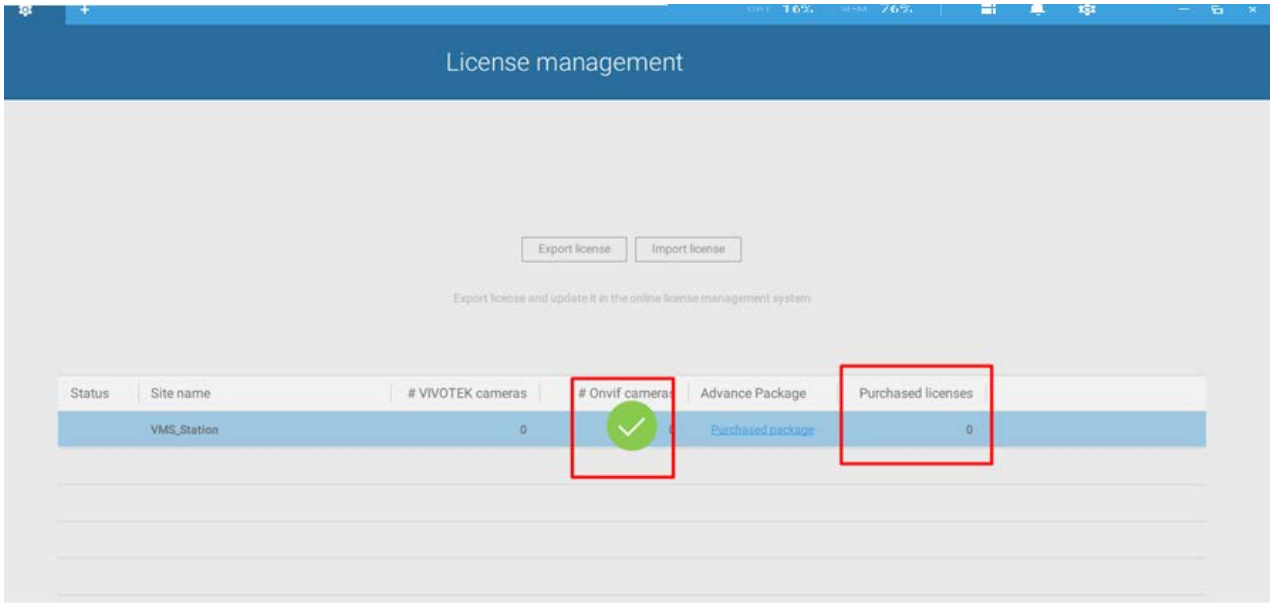
4. How to Import MAC licenses to VAST2

When you acquired the MAC licenses, you can import the licenses to VAST2 using the LiveClient application. You can check the MAC status on the VAST1 server, because VAST2 does not have information for MAC licenses yet.

4-1. Go to LiveClient > Help > license > Import license.

4-2. Select the license file.

4-3. The License management page will display the message of a successful import. The number of purchased licenses will still be displayed.



5. How to Buy More MAC Licenses for Future Distribution?

Chances are users may find it troublesome when their camera deployment expands, and need to purchase more new camera licenses. Assuming that you have 100 cameras, you may only need to buy 68 more MAC licenses because 32 of them are free. You can purchase 100 MAC licenses since you already have those cameras' MAC address, and use the 32 free licenses as backup.

In the event of camera break-down, the replacement camera needs to be activated using another MAC license.

To update MAC licenses for VAST running on virtual machines:

1. Export VAST2 license request from on the virtual machine (VMWare, Hyper-V, etc.)
2. Go to VAST2 license page.
3. Use the Hotkey combination, Ctrl + Shift + Alt + M.
4. Go to the download destination folder to open the MAC file, VAST2Generated_MACList.txt. Copy all MAC addresses. See previous discussion.
5. Contact your sales representatives for the purchase process.

* MAC license is now not tied to PC hardware components and changes to hardware components will not affect the validity of licenses.

Reminders for VAST Software License

Limitations:

1. 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. The licensing mechanism does not apply to machines running Virtualized OSes (**VMWare**, **VirtualBox**, **Hyper-V**, **Parallels**), either through an upgrade or generating software license on a new installation.

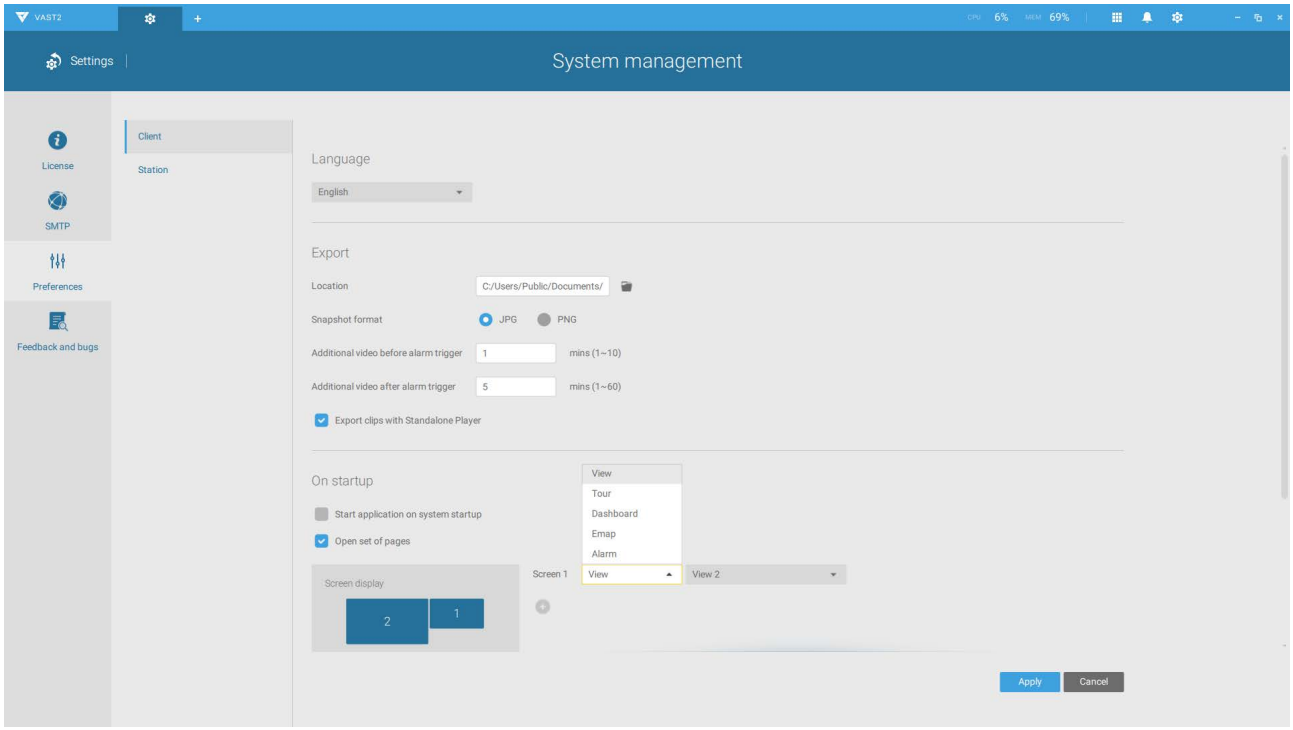
8. If the VAST server is removed and then re-installed, the number of licensed channels remains intact.
9. If users plan to integrate the software licenses from previous dongle licenses, problems may occur if users changed the exported license file name.

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:

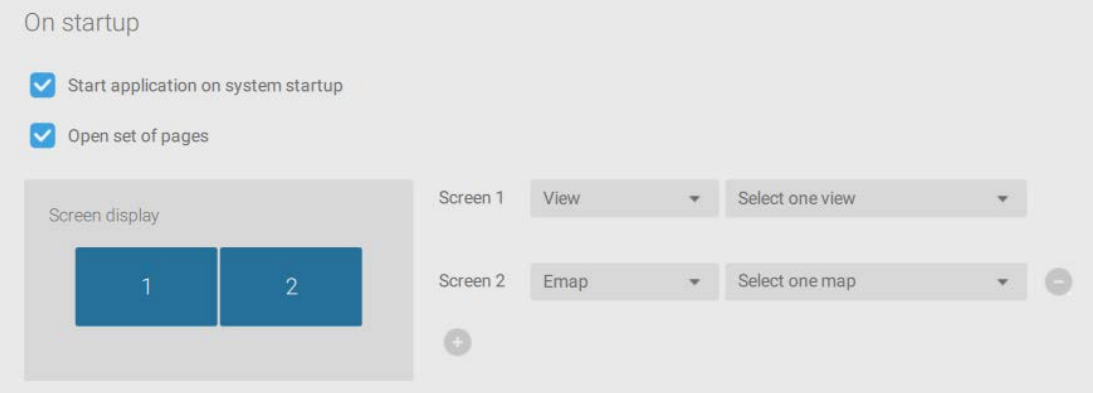
1. Select the UI text language.
2. Configure a default destination for exporting video, snapshots, or configuration backups. The default is "C:\Users\Public\Documents\VIVOTEK Inc\VAST\Downloads". You can change the media format via the checkboxes.
3. Select the format for the snapshot as either JPG or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



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.



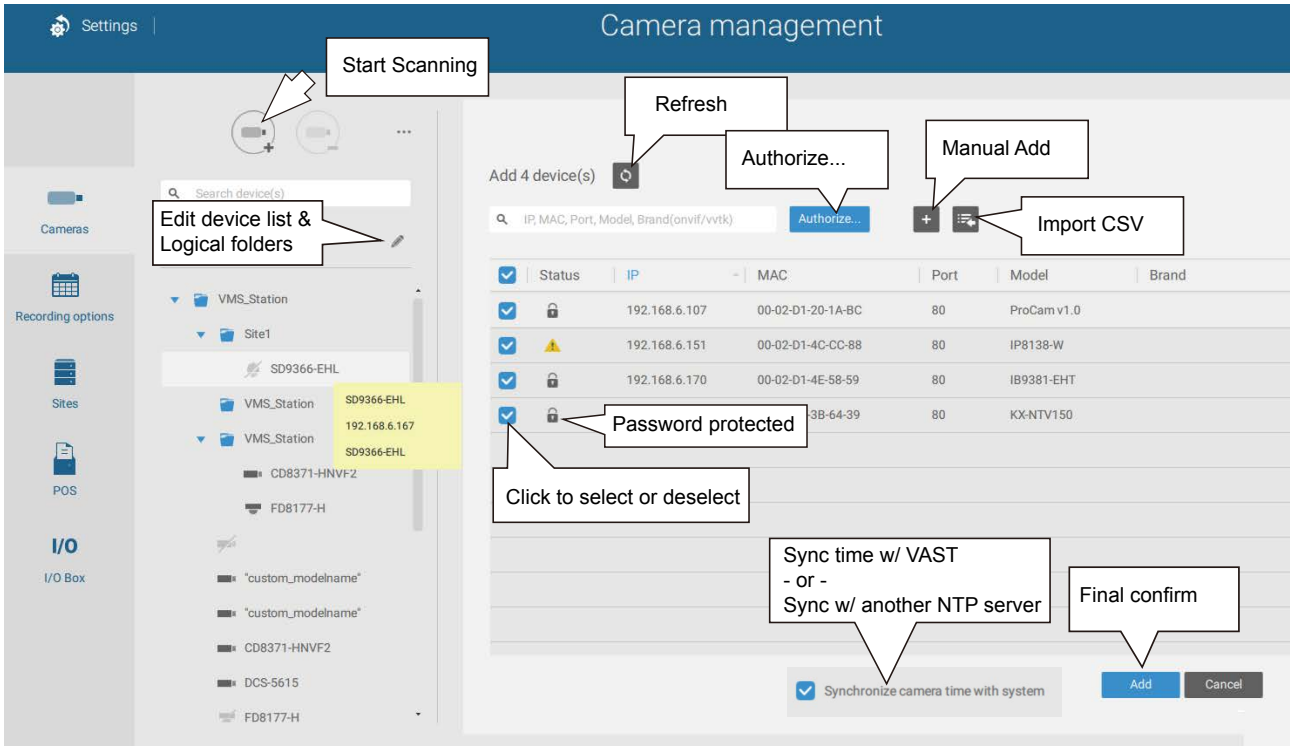
Station Setting:

1. 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.
2. Log: Use the menu to configure the preservation time of the Major, Normal, or Minor logs.
3. Bookmark: Configure the days of preservation for bookmarks.
4. Trend Micro events: Configure the days of preservation for events related to cyber security.
5. 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.



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 pre-configured 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.

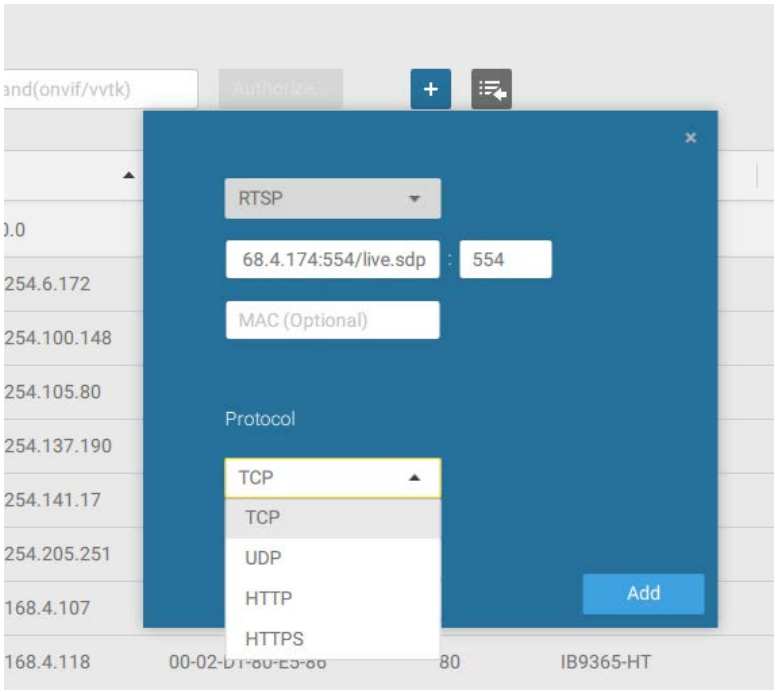
- Retrieve RTSP streaming on specific port: The default port for RTSP streaming is 554. If you want to change this port, please check this item and fill in a desired port number.

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."



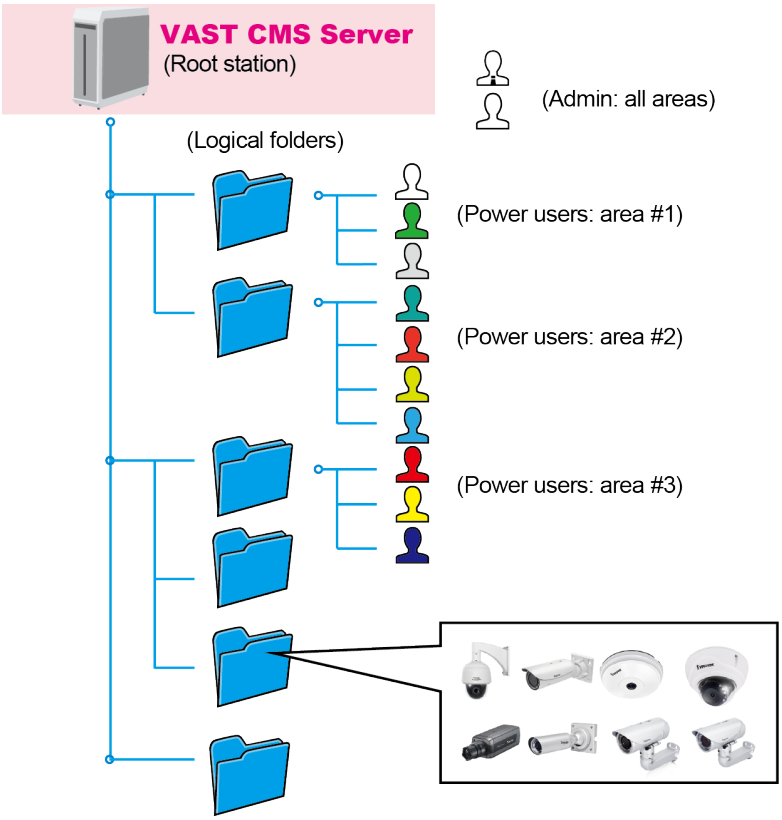
2. Enter the camera's IP address.
3. Enter the camera's MAC address as printed on the camera label, or one found by the Shepherd utility.
4. Enter "554" in the Configuration port.
5. Enter "live.sdp" in the URL field, as this is part of the original RTSP streaming command: "rtsp://172.18.204.58:554/live.sdp". 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.

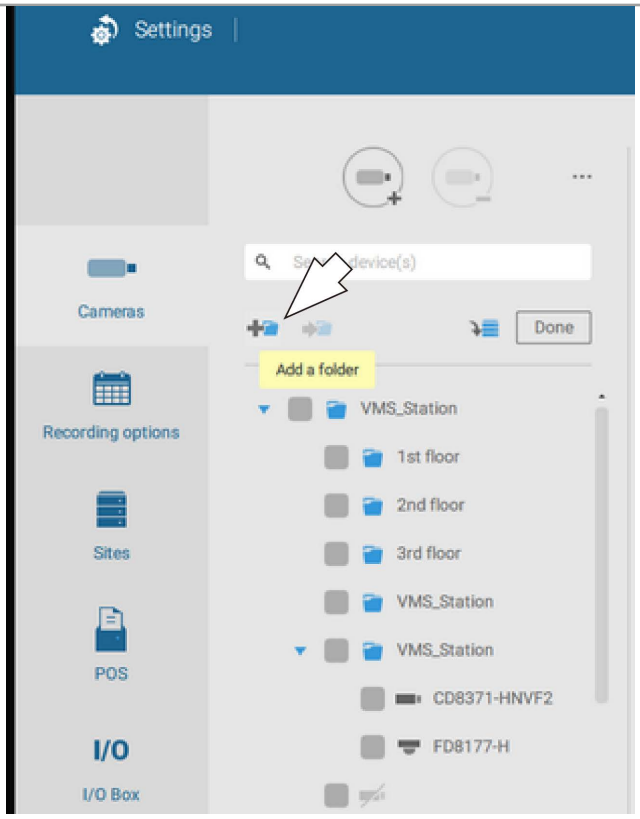
4-3. Logical Folders

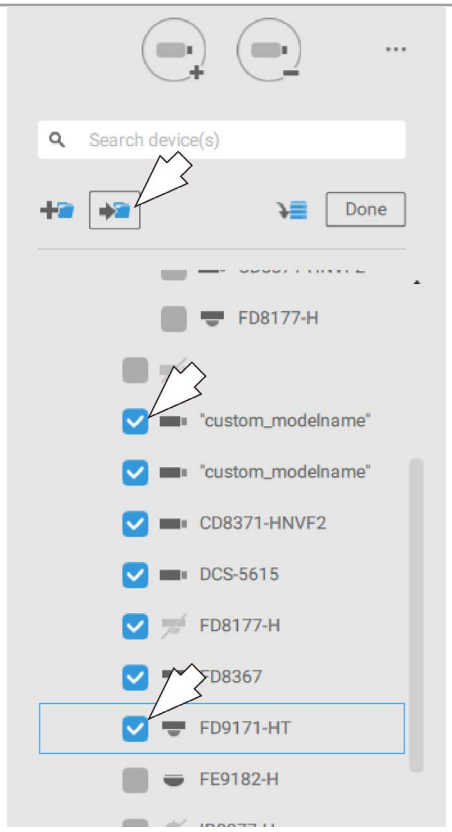
The Logical Folders allow you to re-define the logical relationships between the real-world deployment and the physical devices (cameras). For example, according to your deployments, you can designate several cameras to be listed under a logical sub-directory named as "Building A," and the other cameras into "Building B." In this way, you can re-arrange your cameras and devices on a tree view that is geographically more accurate.



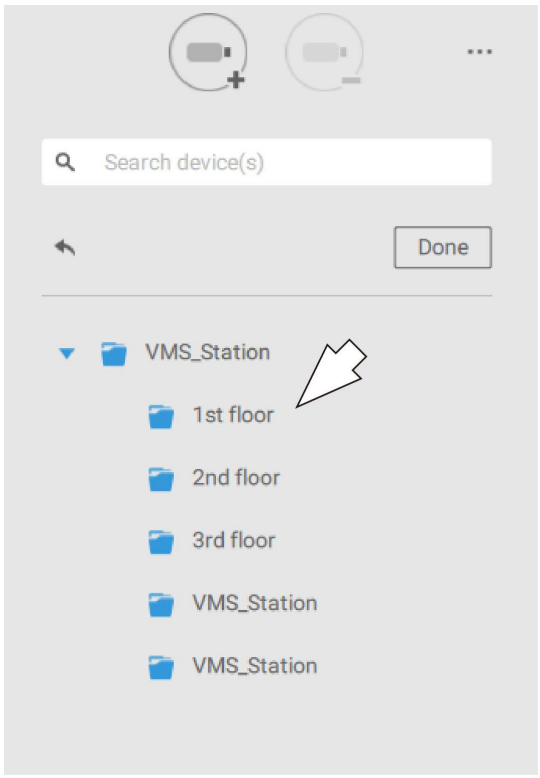
To create logical folders,

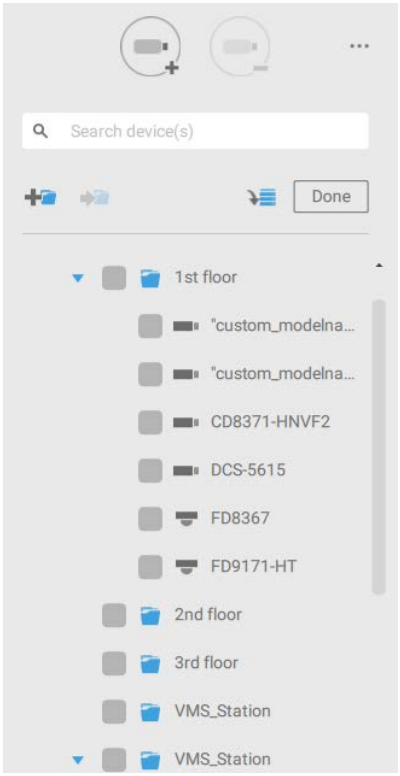
1. On the Settings > Cameras page, click the Edit button.
2. Click on the Add a folder button.
3. Enter a name for the folder, e.g., 1st floor, 2nd floor,... according to your needs as shown below.
4. Repeat the process to create more folders.
5. Make sure you enlisted all cameras in your deployment. You can start moving cameras to specific folders. Click on the Move Selected Items button.



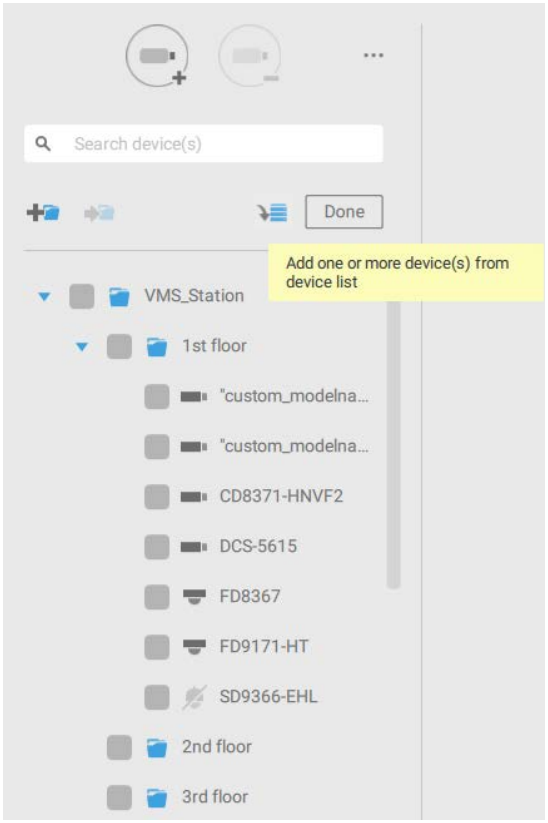


6. Select a logical folder to move the devices to. The selected devices will be listed under the logical folder you selected. Repeat the process to move cameras to each logical folder.

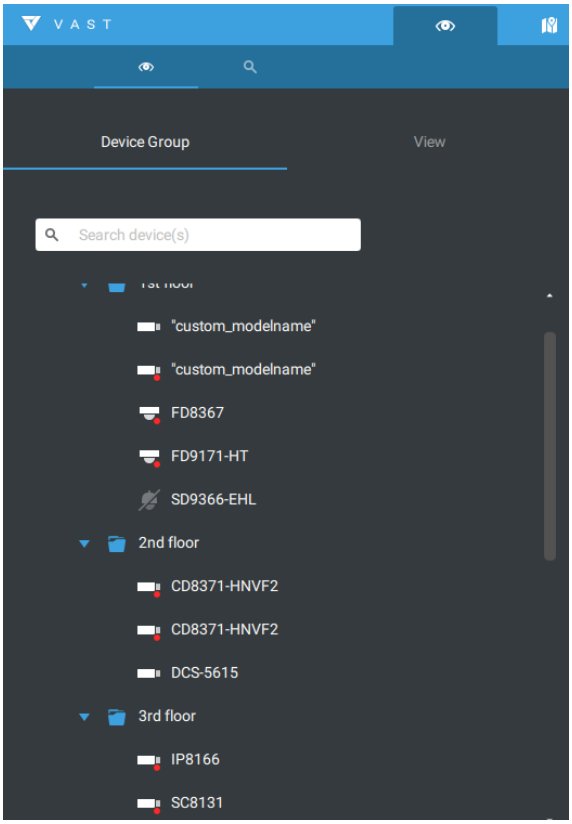




You can also use the add device button to select devices from the list and move them to a specific folder.



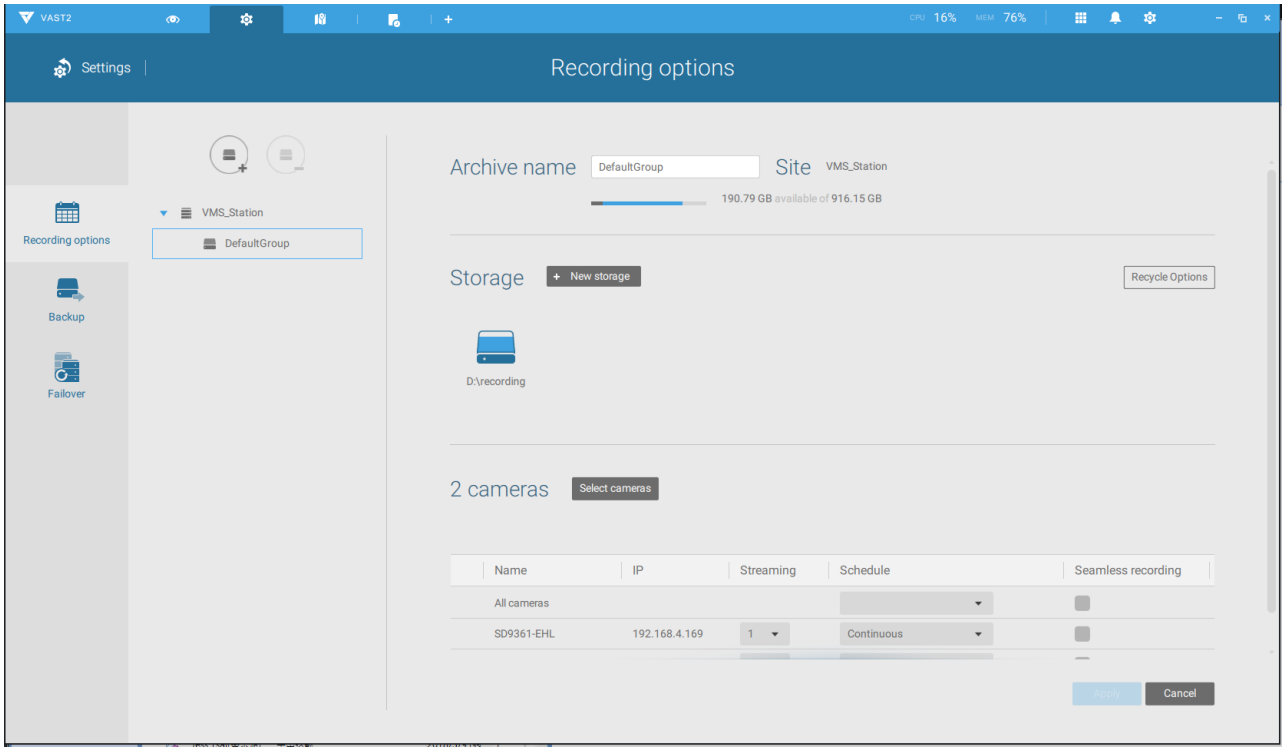
Return to live view, and you can see the configuration change takes effect.



4-4. Settings > Recording > Recording Options

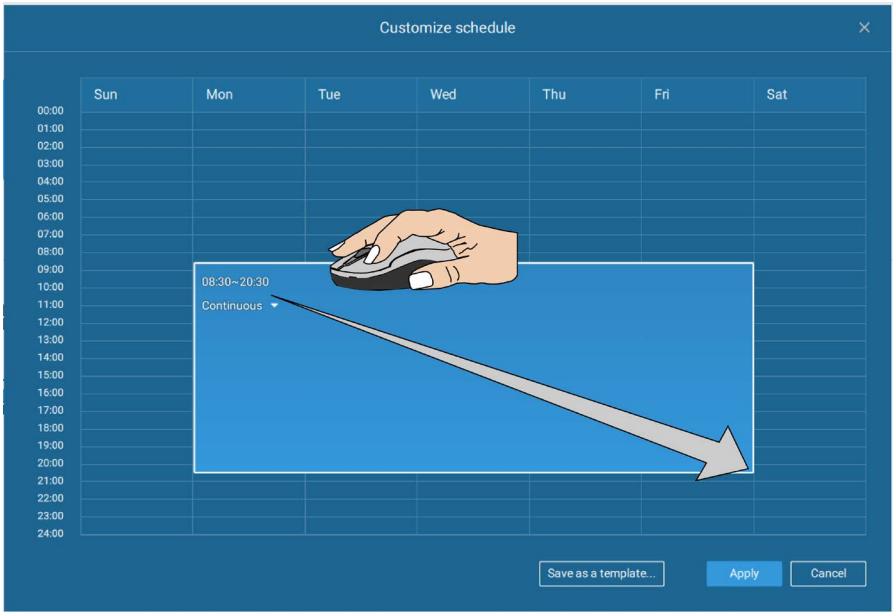
Click Settings > Recording options. The Recording options window will prompt.

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



Click on any of the options on the Schedule panel for a recording option: Continuous recordings, Events only, None, or Customize.

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.

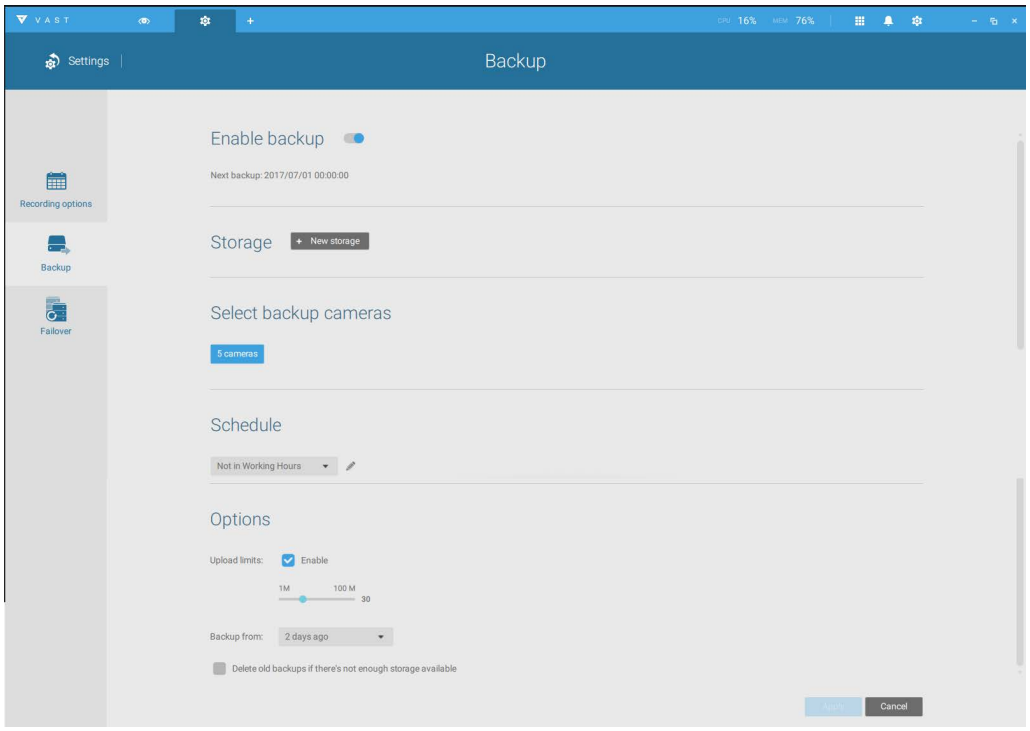
The same configuraion window apply to both the Schedule template and the customize schedule windows.

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

4-5. Settings > Recording > Backup

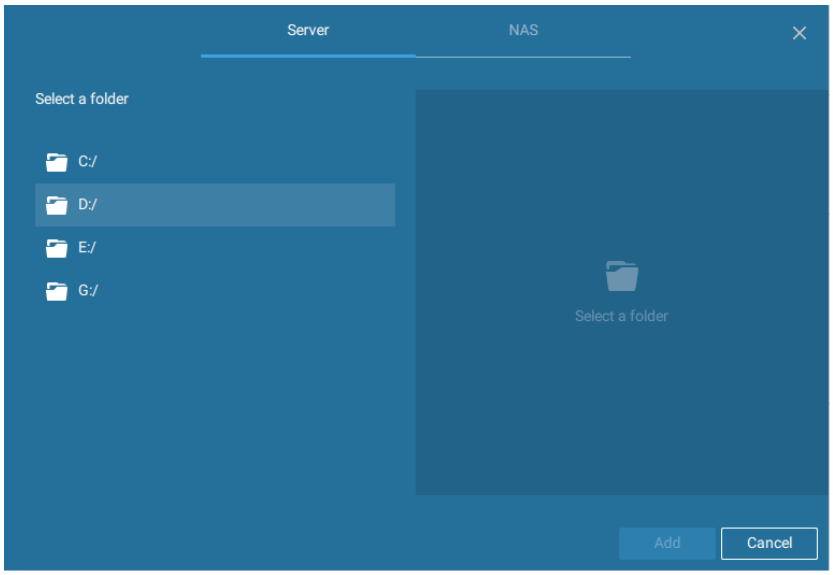
The Backup function allows you to regularly back up the video recordings of one or multiple cameras to local hard disks or a Network Attached Storage device. Currently, the VAST2 server does not support backup to external storage devices such as a storage devices connected via Fibre Channel. VAST supports 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.

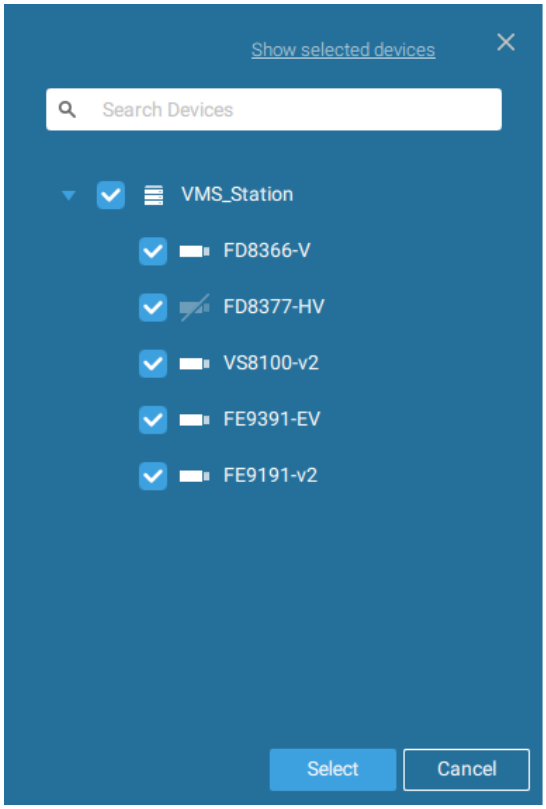


To enable a backup schedule,

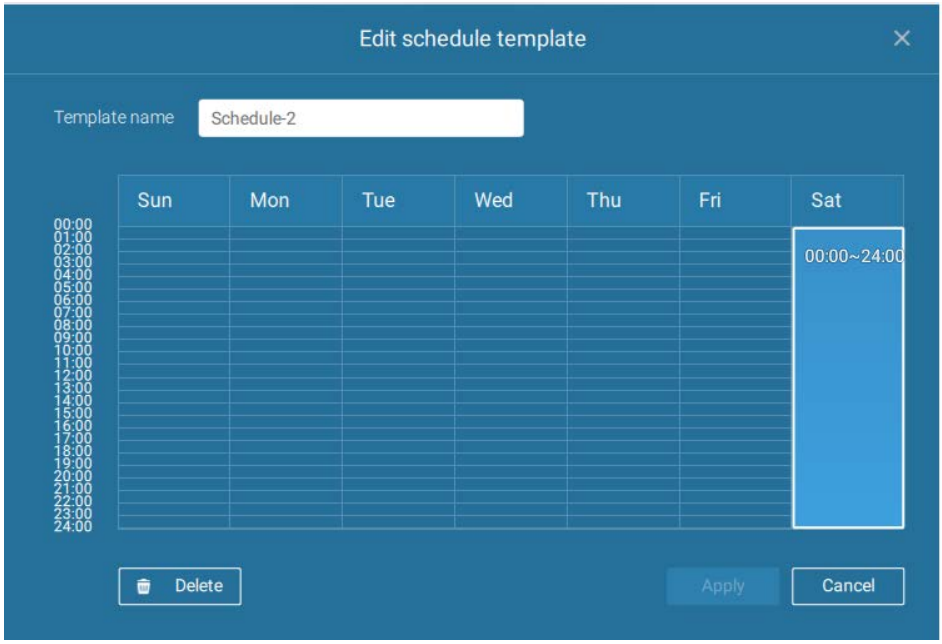
1. Enable the backup by selecting the "Enable backup" slide switch.
2. Click to add New storage. A configuration window will prompt showing all accessible storage. Click the NAS tab to enable access to a network share.



3. Select the cameras whose videos will be backed up.

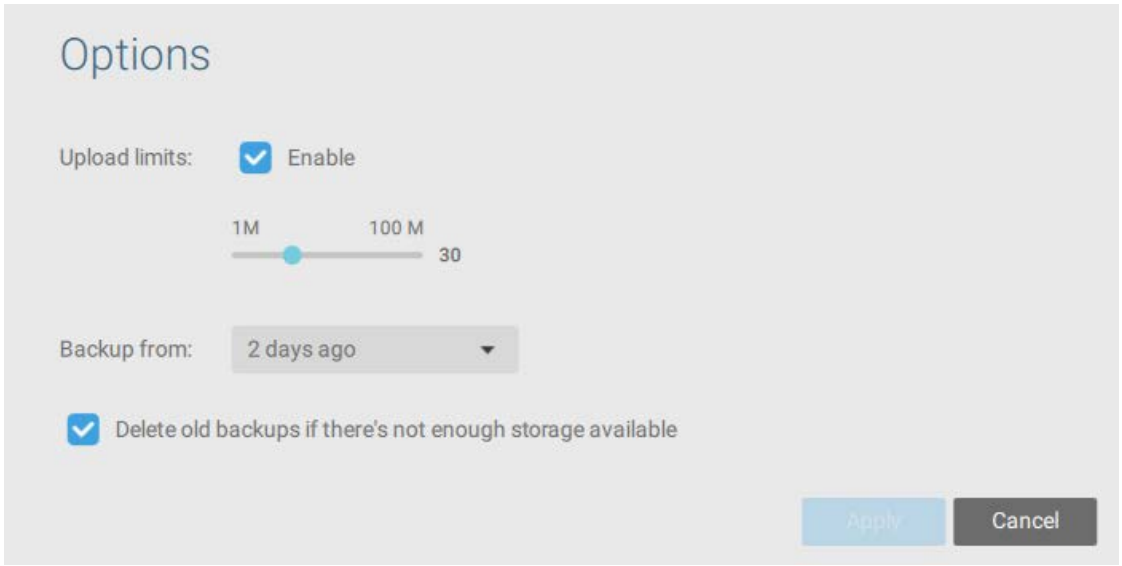


4. Select or configure a new schedule template for the backup process to take place. You can select a time when the network load is low, such as the off-office hours, to avoid network congestions.



5. On the Options pane, you can configure an upper bandwidth threshold (in Megabytes) for the backup operation (for all selected cameras/channels).

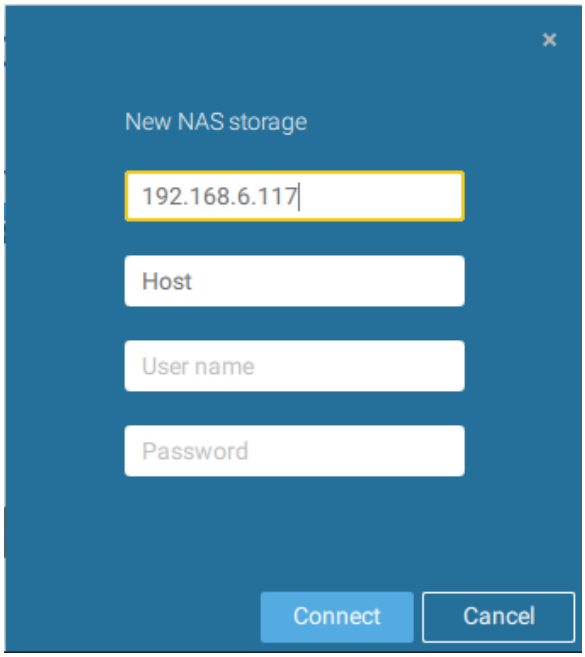
   You can select the extension of time, such as starting from how many days ago, of your backup task. You can select to remove old backups when you run short of storage volume.

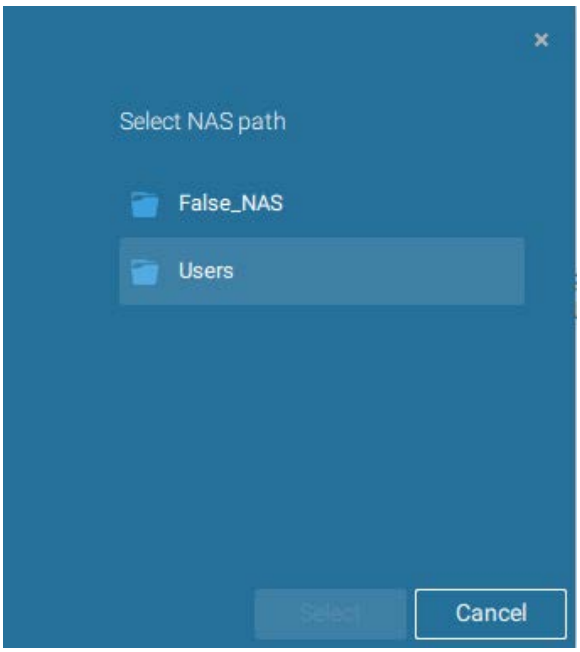


Storage

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.





Select storage volumes each by a single click.

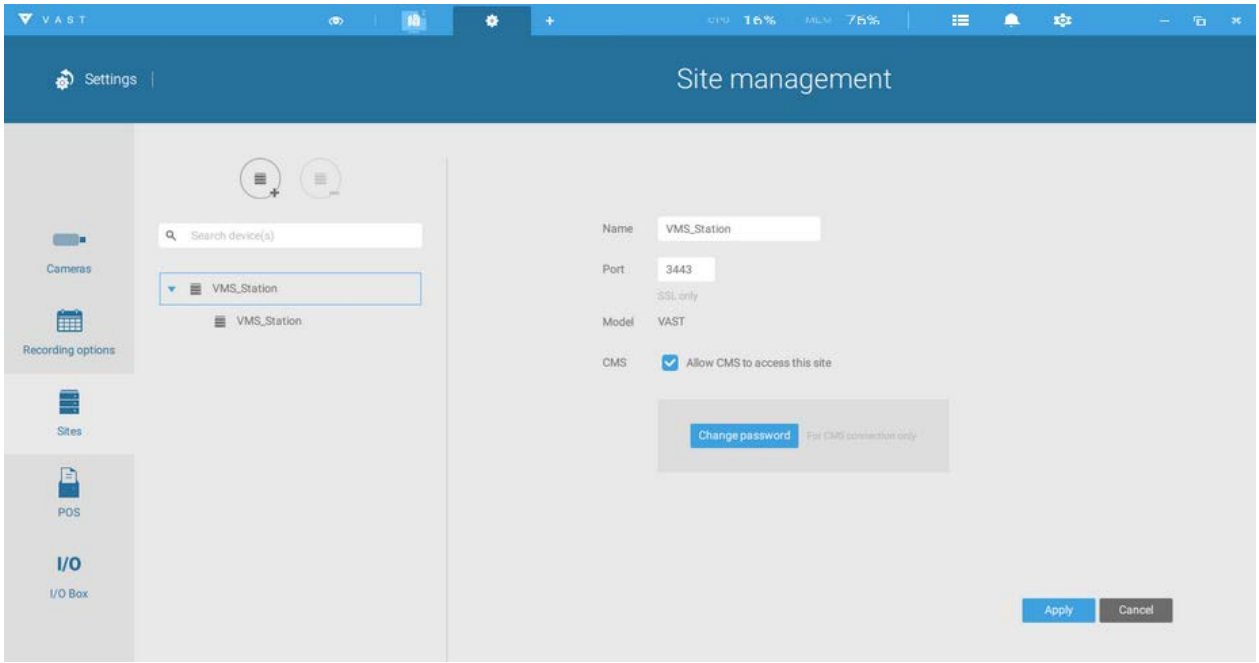
Click **Ready to use** to continue.

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.

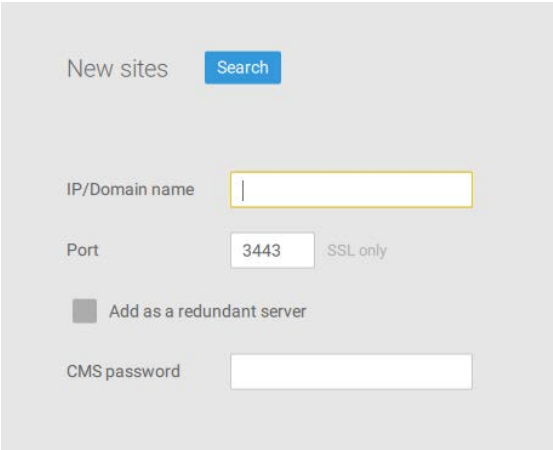
Each individual VAST station manages its own surveillance deployments. To build a hierarchy, proceed with the following:

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.

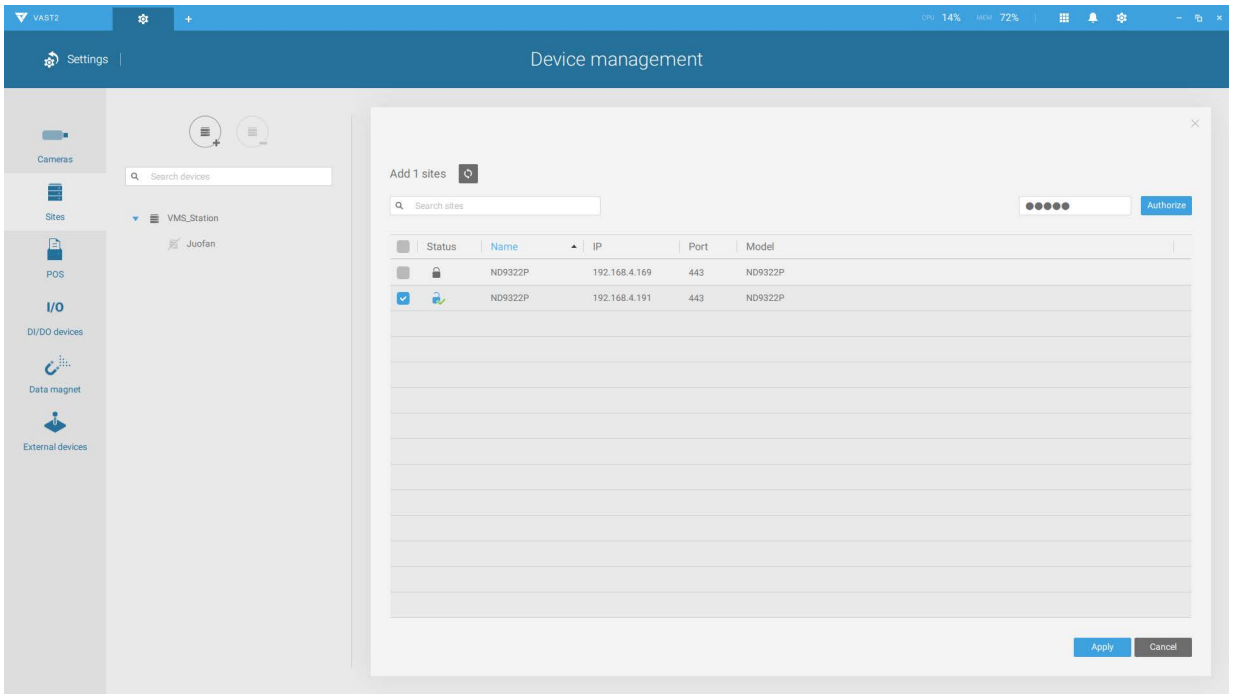


6. Click the Apply button.
7. Open the VAST 2 client on the server chosen as the CMS.
8. Click the Add sites button.

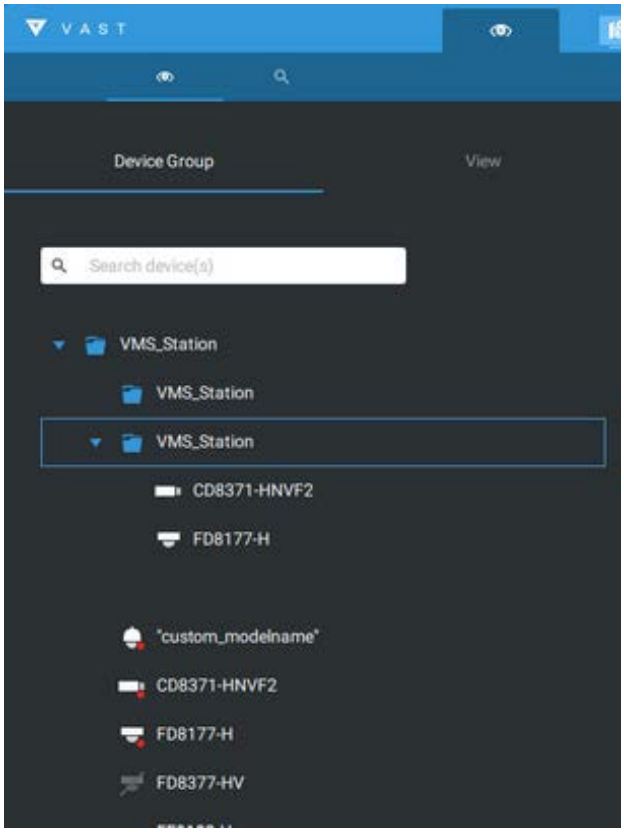
9. You can click the Search button if the sub-station is reacheable in a local network, or manually enter the IP address, and password for making the connection.



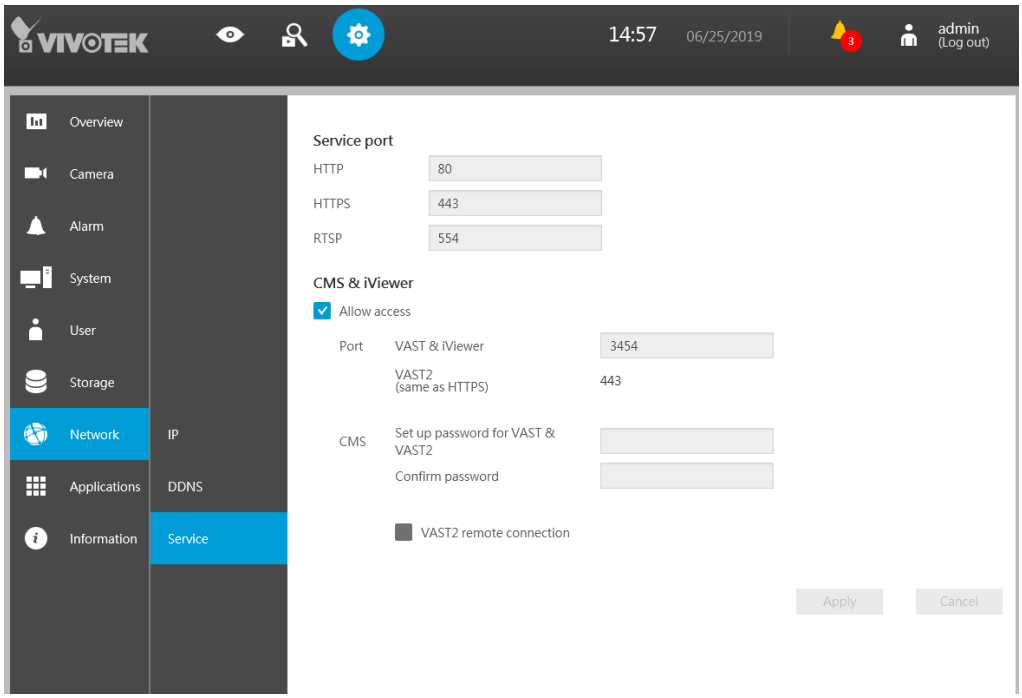
10. Enter the password you configured for the Sites configuration, and then click the Authorize button.
    Click the Apply button for the configuration to take effect.



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.



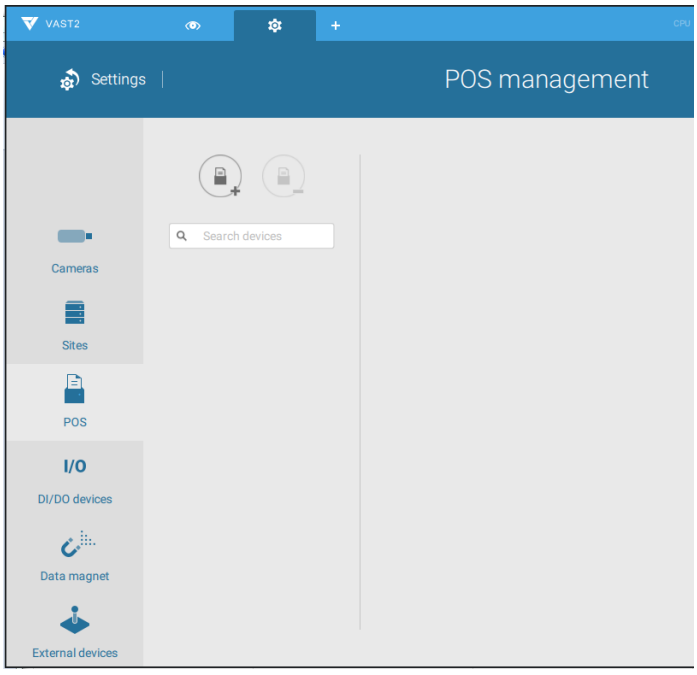
When you want to enlist an NVR into your configuration, please remember to enable the access from VAST server in the NVR's Service page.
The connection between VAST and NVR is made via encrypted https.
If the connection port is changed to a non-SSL port, the access from VAST to NVR will fail.
For adding the ND series NVR, use port 443.

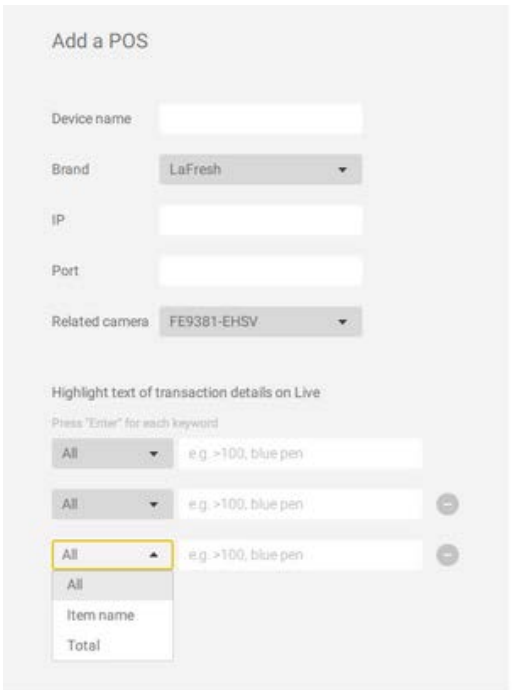


4-7. Settings > Device > POS

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.
2. 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.



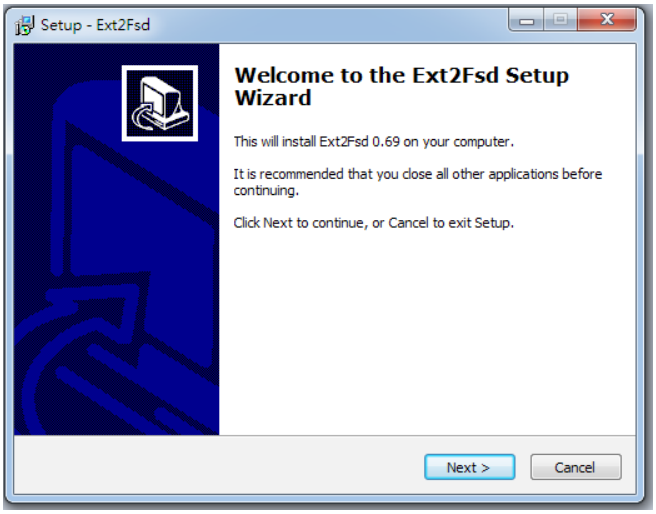


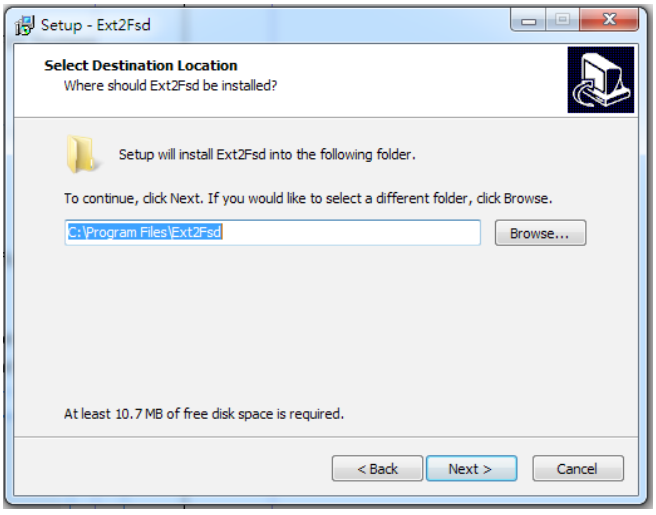
4-8. Settings > Device > Local DB

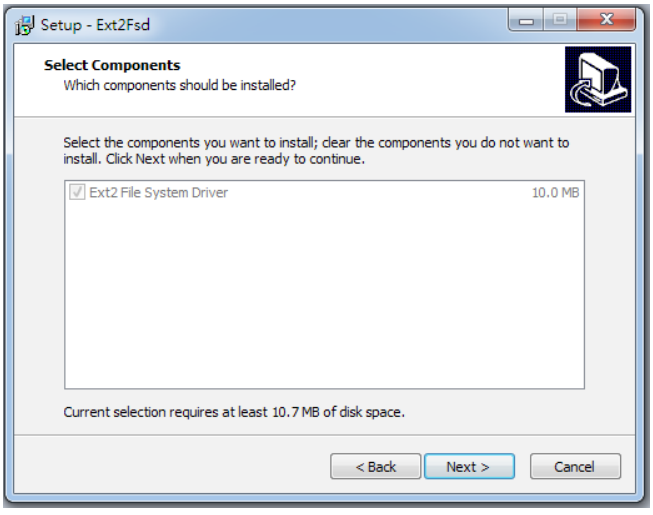
Since some of VIVOTEK's NVRs runs on Linux, you have to install the Ext2 File System Driver for Windows to access the recording files from a NVR hard disk.

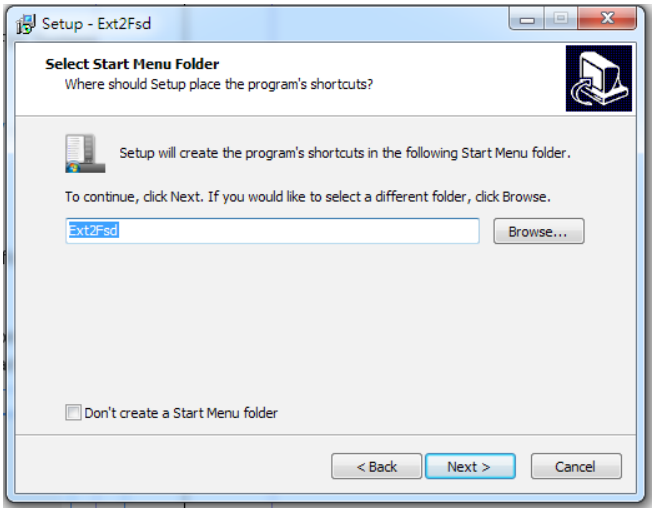
The file system driver can be found here: https://sourceforge.net/projects/ext2fsd/?source=typ_redirect

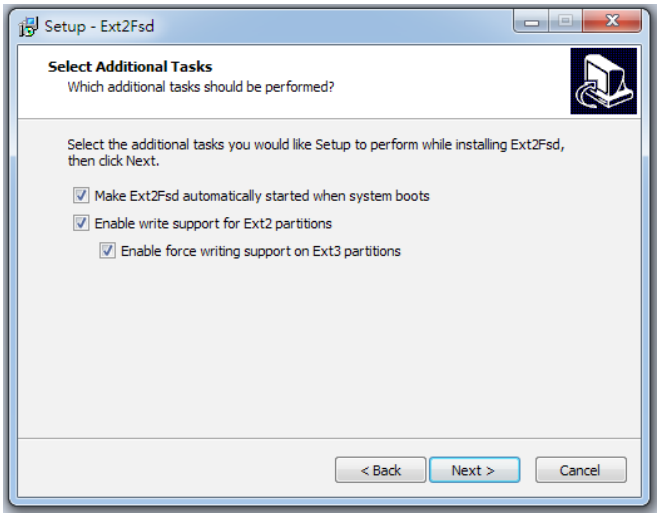
Run and install the Ext2fsd-0.xx.exe. Follow the onscreen instructions to complete the installation.

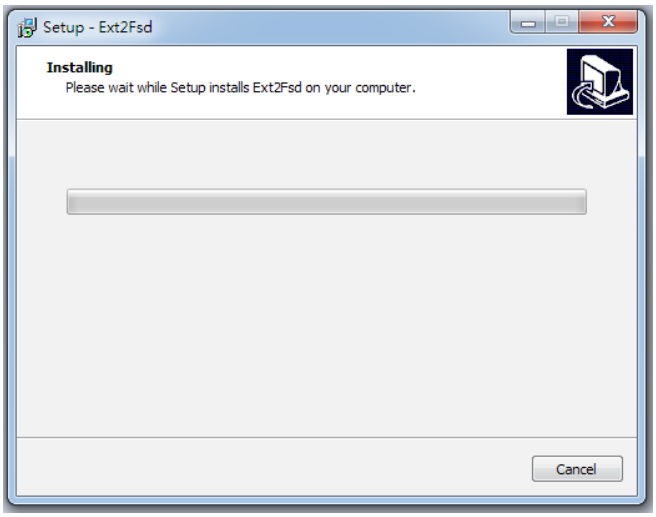


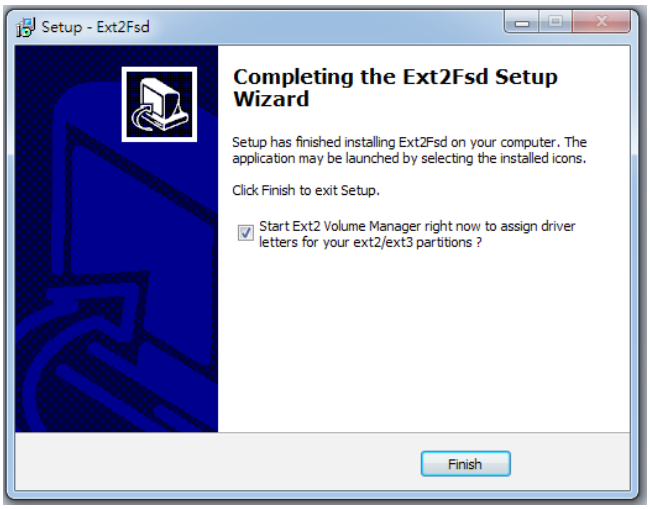


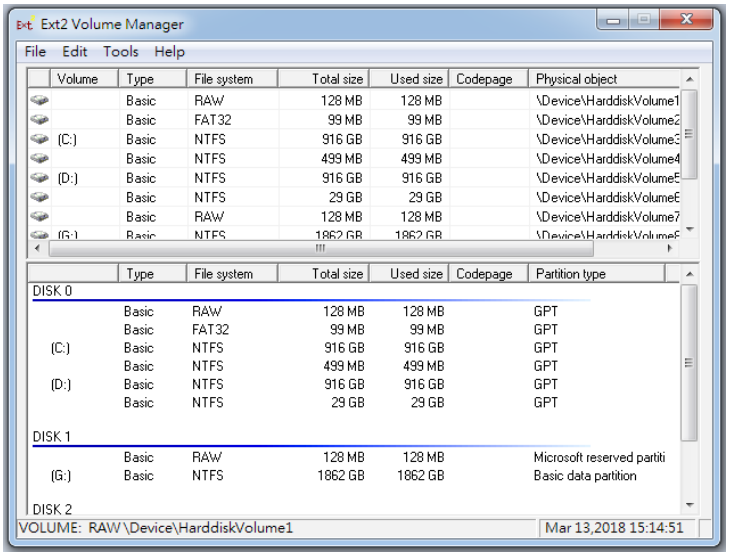



Setup - Ext2Fsd
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Ext2Fsd
Browse...
Don't create a Start Menu folder
< Back
Next >
Cancel

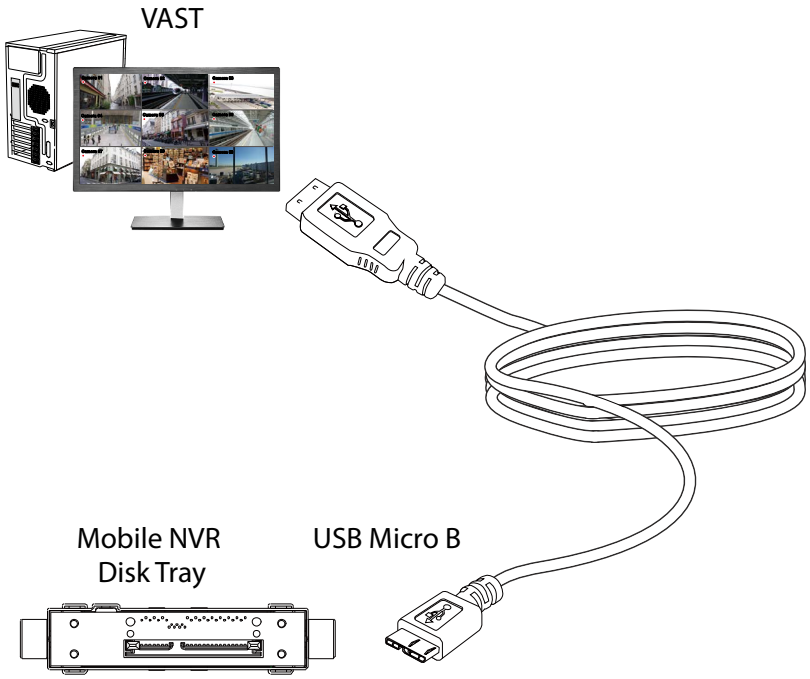

Setup - Ext2Fsd
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing Ext2Fsd, then click Next.
Make Ext2Fsd automatically started when system boots
Enable write support for Ext2 partitions
Enable force writing support on Ext3 partitions
< Back
Next >
Cancel


Setup - Ext2Fsd
Installing
Please wait while Setup installs Ext2Fsd on your computer.
Cancel

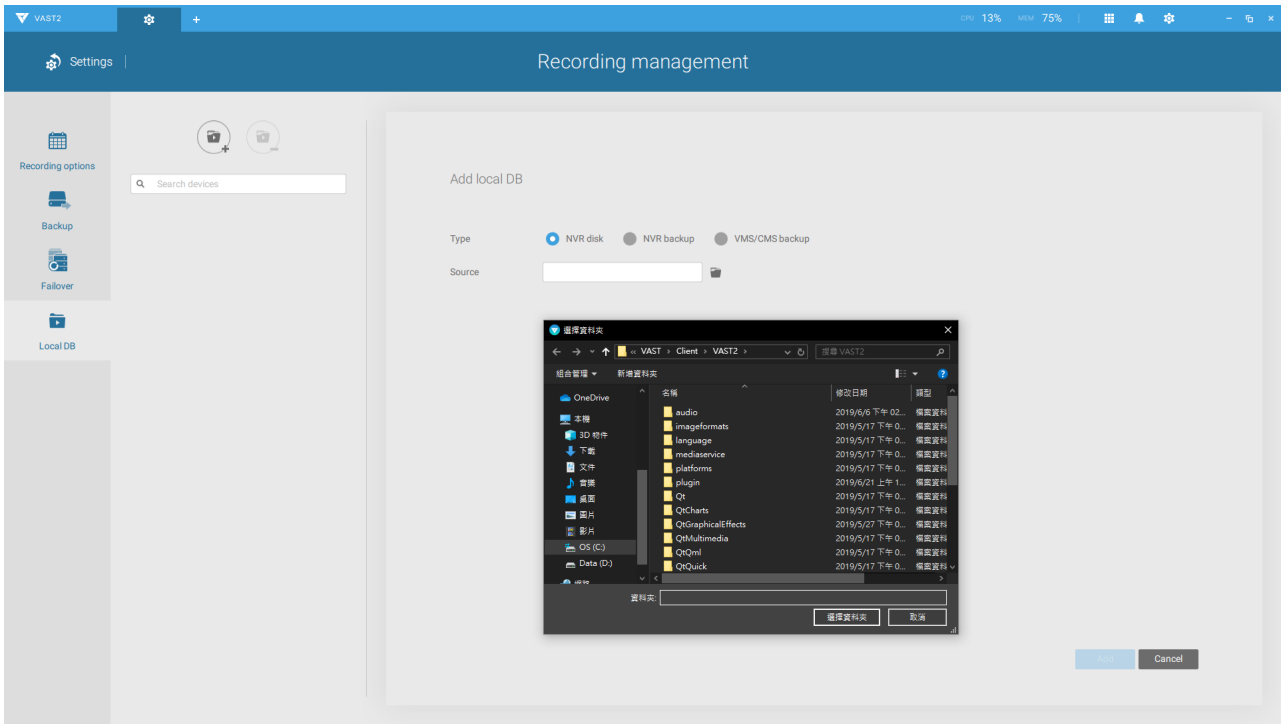

Setup - Ext2Fsd
Completing the Ext2Fsd Setup Wizard
Setup has finished installing Ext2Fsd on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Start Ext2 Volume Manager right now to assign driver letters for your ext2/ext3 partitions ?
Finish


Ext2 Volume Manager
File Edit Tools Help
Volume Type 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\HarddiskVolume6
Basic RAW 128 MB 128 MB \Device\HarddiskVolume7
Type 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
DISK 1
Basic RAW 128 MB 128 MB Microsoft reserved partiti
(G:) Basic NTFS 1862 GB 1862 GB Basic data partition
DISK 2
VOLUME: RAW \Device\HarddiskVolume1
Mar 13,2018 15:14:51

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.

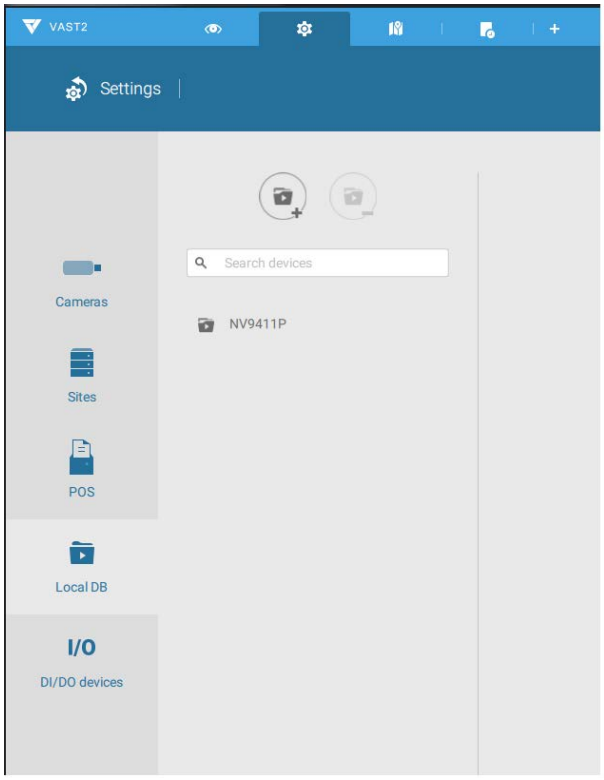


3. From VAST, enter **Settings** > **Device** > **Locabl DB**.
4. There are 3 import types:
   1. **NVR disk**: the drive tray box removed from a mobile NVR.
   2. **NVR backup**: the recorded videos exported from an NVR using a USB thumb disk or portable drive.
   3. **VAST backup**: scheduled backup from the local machine. They include: VAST backups from previous software releases, and scheduled backups.

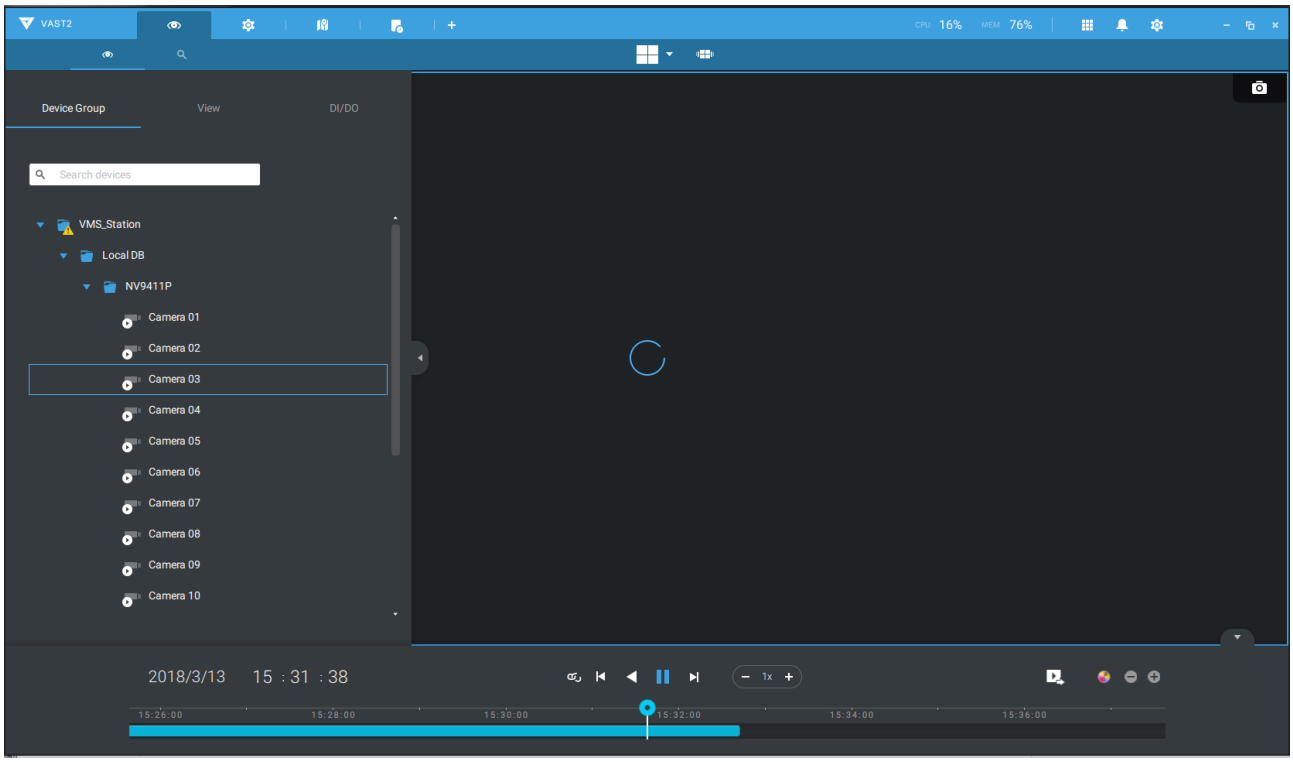


5. Taking a mobile NVR's disk drive as an example, click the Source select button to locate the disk drive.

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 

. 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.

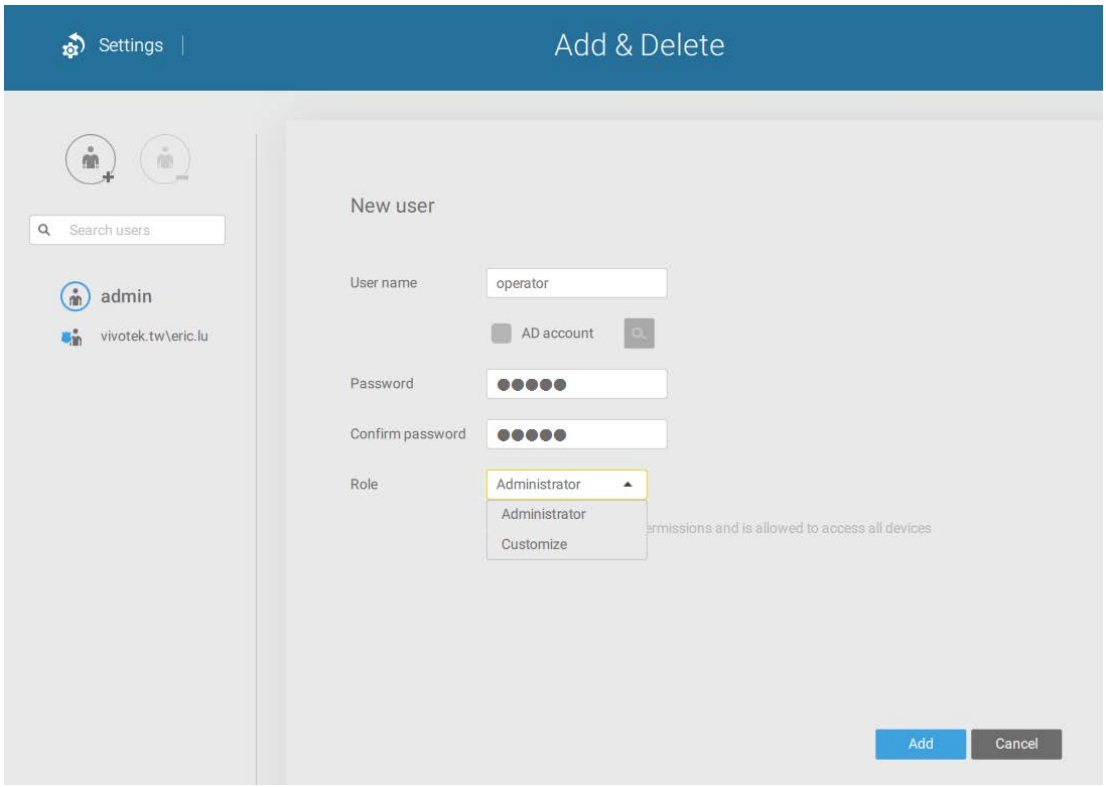
4-10. Settings > IO Box and Related Configuration

Please refer to page 129 for information.

4-11. Settings > User Management

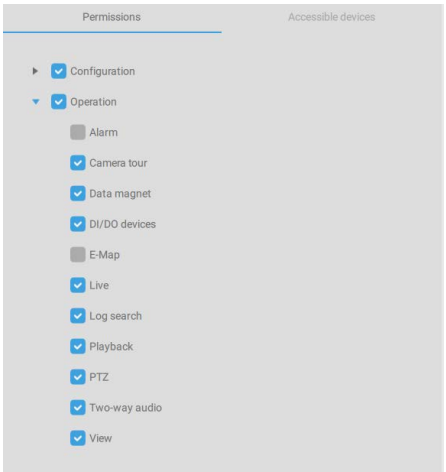
The User Add & Delete page allows you to create users with the permissions for different operational capabilities.

To specify the authorized privileges, select Customize in the Role menu, then select the Permissions and/or the Accessible devices tabbed menus.

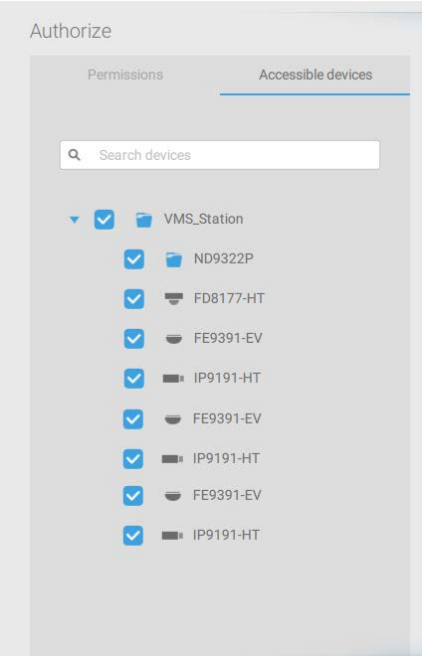


Use the Customize option to limit the authorized actions of a user.

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

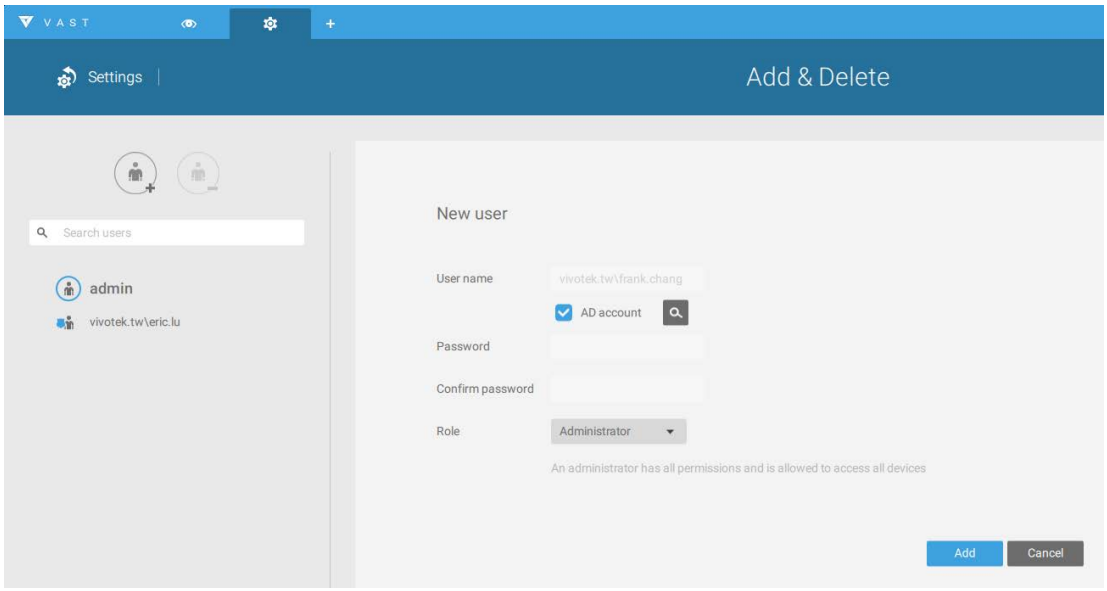
In an established, enterprise network environment, the support for Windows AD (Active Directory) infrastructure enables ease of integration using the credentials of existing users. Using the same AD authentication methodologies, you can configure the clients or users in an established network to access 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.
8. The userPrincipalName of your Windows AD account can be different from the sAMAccountName. However, You can only use the sAMAccountName to login VAST 2.
9. The userPrincipalName field of your Windows AD account should not be empty.

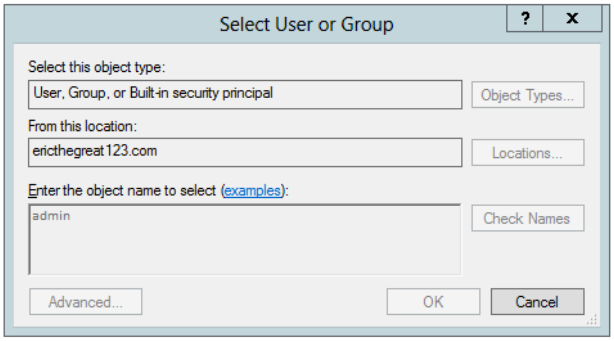
To add an existing AD user,

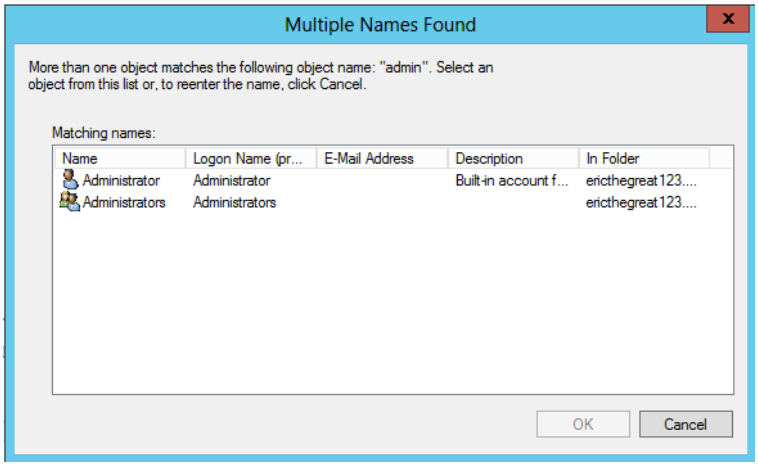
1. Select the AD account checkbox.



2. Click the Search button.

3. Enter a user name or group name to search, e.g., Frank. Click OK when done.

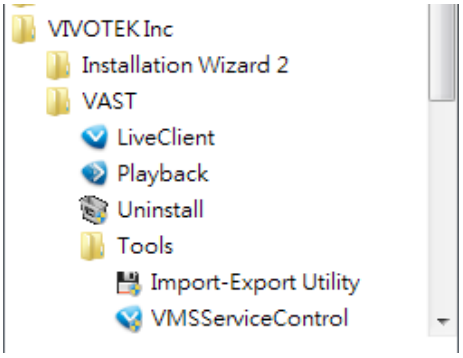




4. Enter the password twice for the AD user.
5. Select the privilege role for the user, configure his/her privilege settings as described above and then click Add.

Appendix A: VAST Service Control Tool

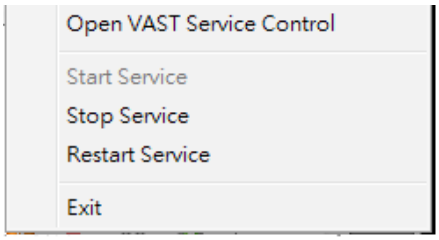
VAST service control tool is a tool for server control and for user to be aware of the VAST Server status. It starts up as Windows OS startup.
Under Microsoft Windows, choose "**Start > VIVOTEK Inc VAST > VMServiceControl.**"

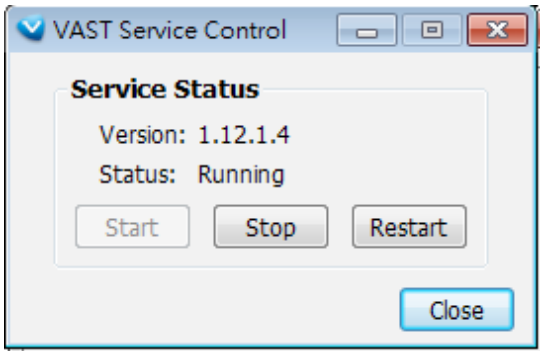


You may also find it in the system tray icon of the tool bar, which indicates that the service is running: 

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:

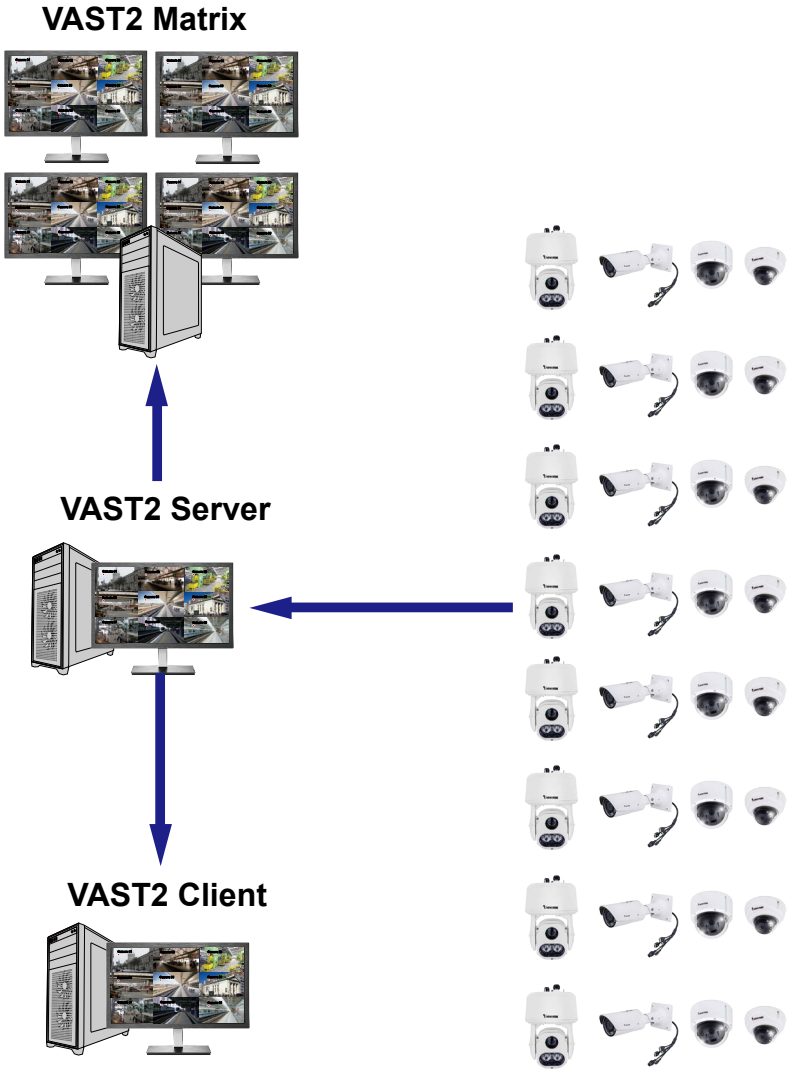




Here you can manually start, stop and restart the service.

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.

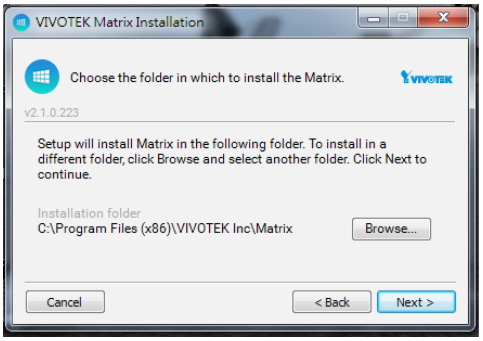


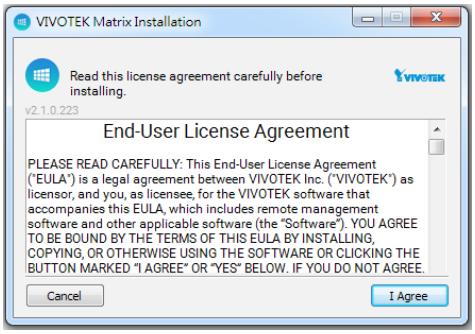
Prerequisites:

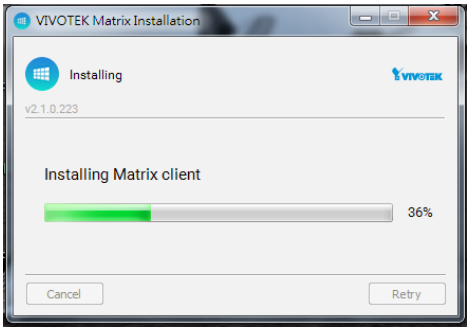
1. One VAST2 server and another computer running the Matrix client utility.
2. The first 2 digits of software revision numbers of VAST server and Matrix client must be the same: e.g., 2.3.x.x and 2.3.x.x.
3. Sufficient network bandwidth among network cameras, VAST servers, and Matrix clients.

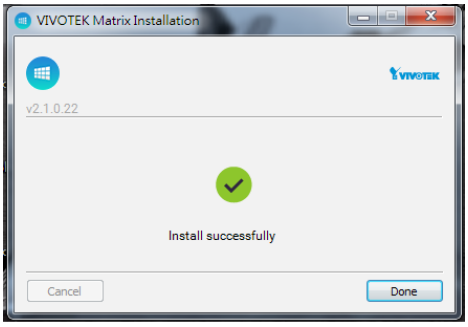
Configuration procedure:

1. Install the Matrix client utility on a computer equipped with multiple monitors. Follow the onscreen instructions to install the utility.

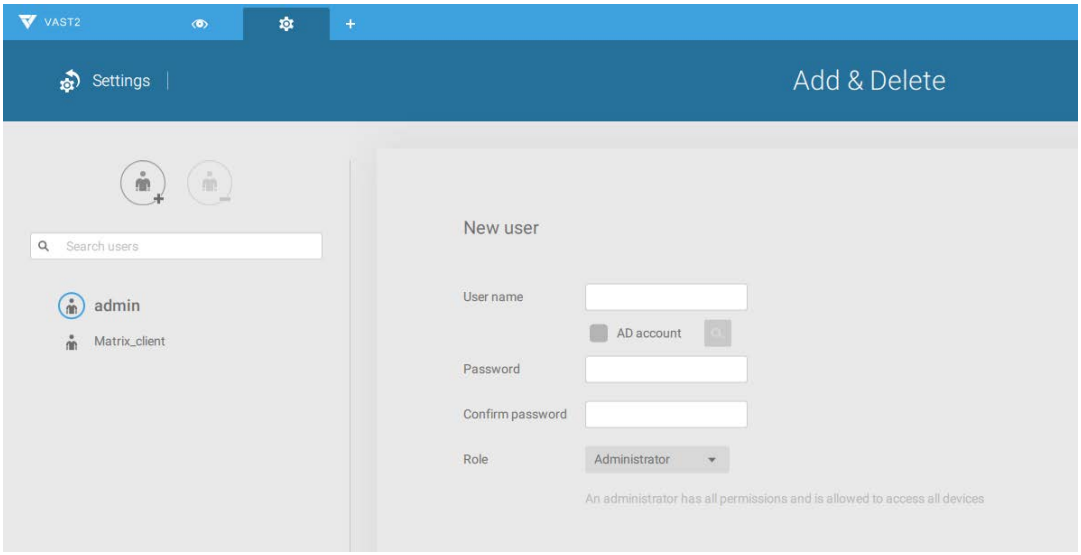




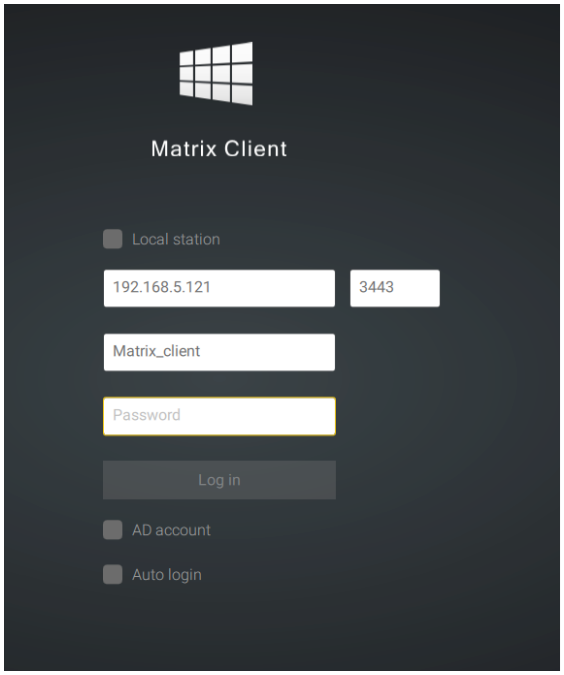




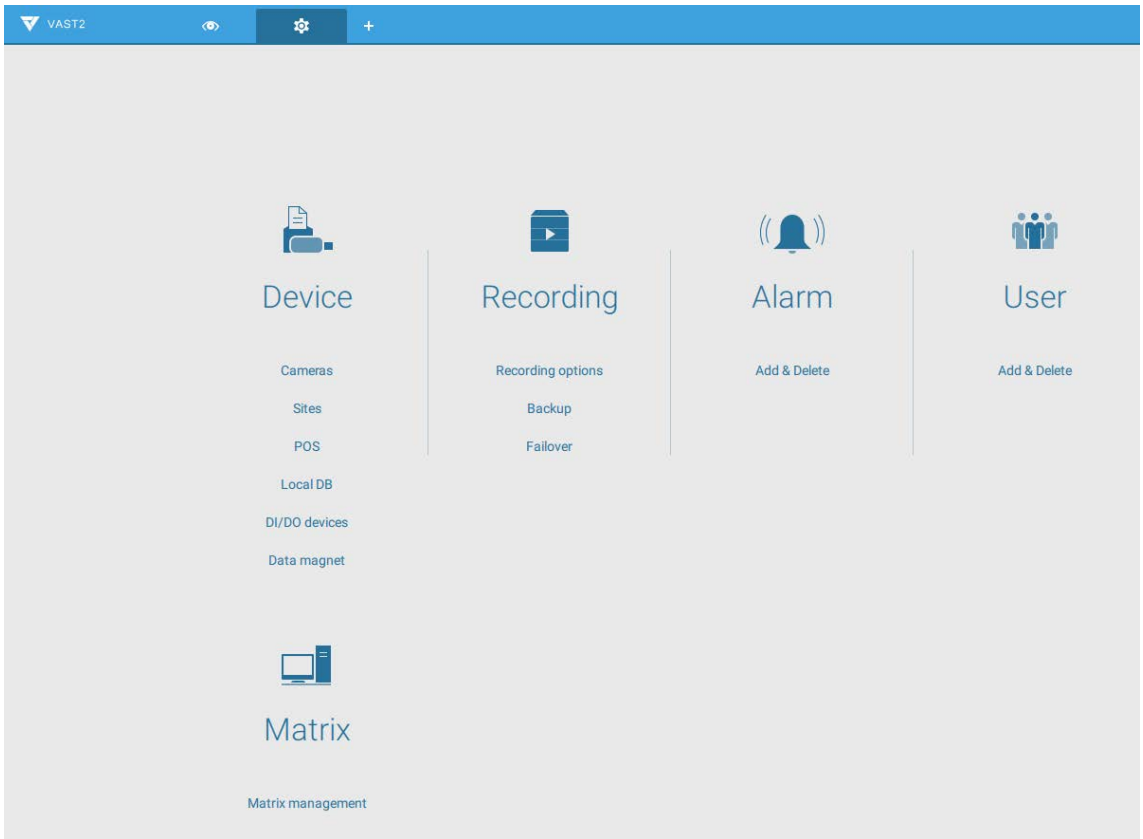
2. On the VAST server, create a user account for the Matrix client. Depending on the operation on the client computer, assign the client user with adequate operation privileges.



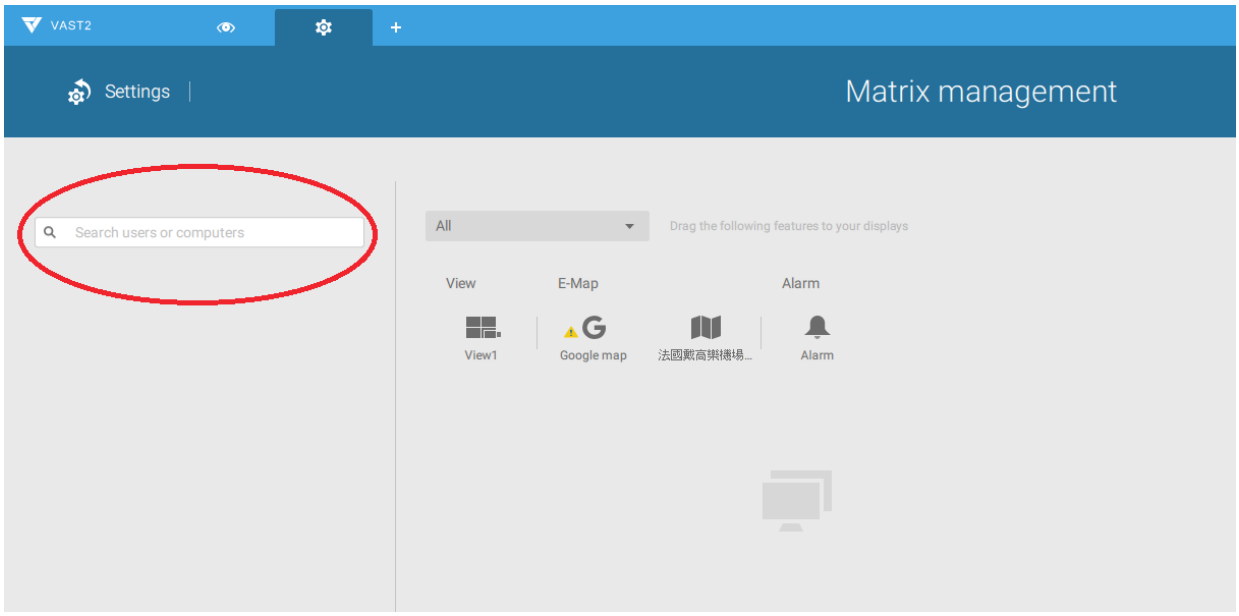
3. Open the Matrix utility, log in to the VAST server address, using the Matrix client account credentials.



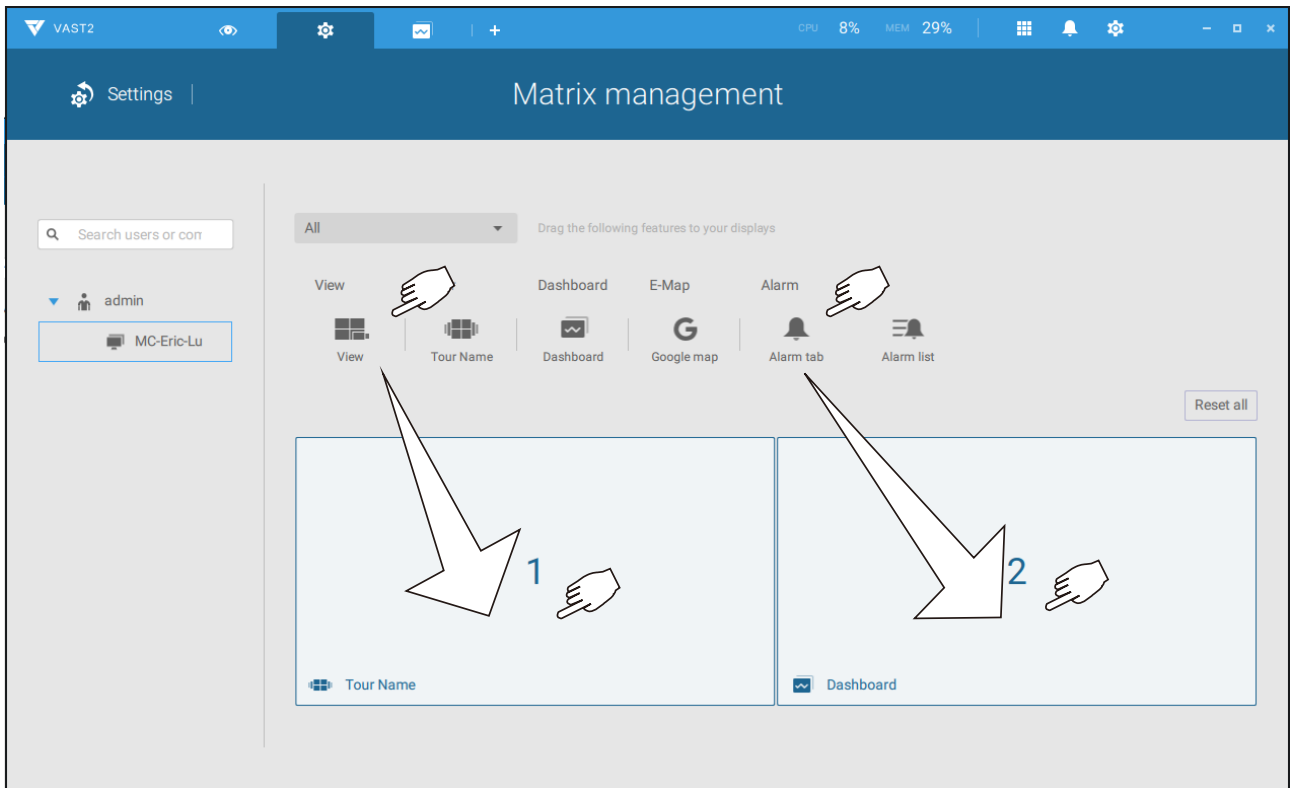
4. From the VAST server, open the Settings > Matrix Management window.



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).

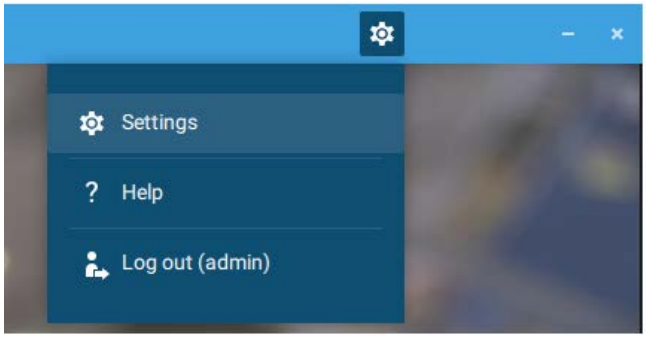


6. Once the VAST server found the Matrix client, the available monitors will be listed. Click and drag the pre-configured Views, Tour, Dashboard, E-maps, or Alarm panel to any of the monitors.

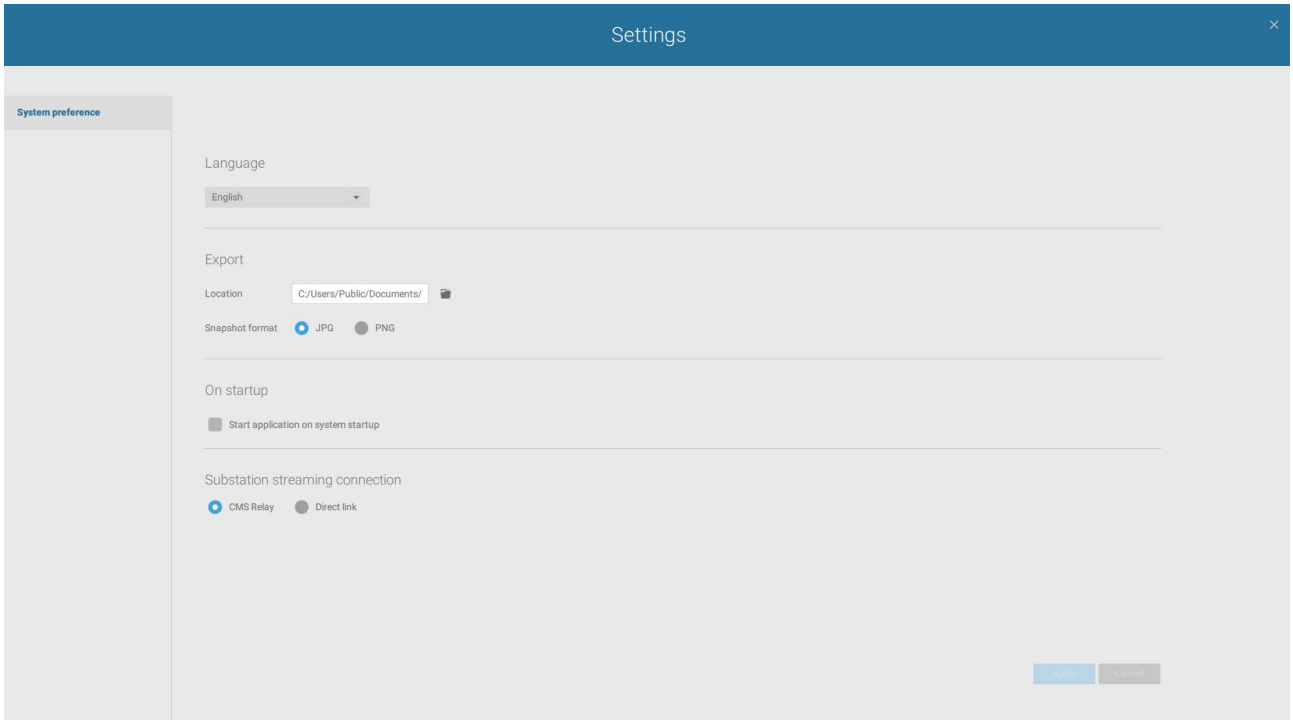


7. The views should immediately appear on the Matrix monitors.

8. If you need to log out, move your mouse cursor to the top of the Matrix client screen to end the session.



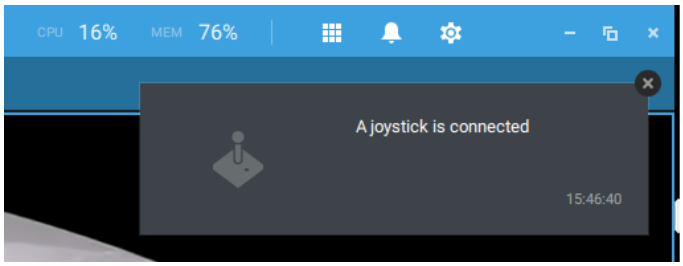
If necessary, change your client settings. Here you can change the displayed language, Export target folder, Start-up option, and the streaming connection options.



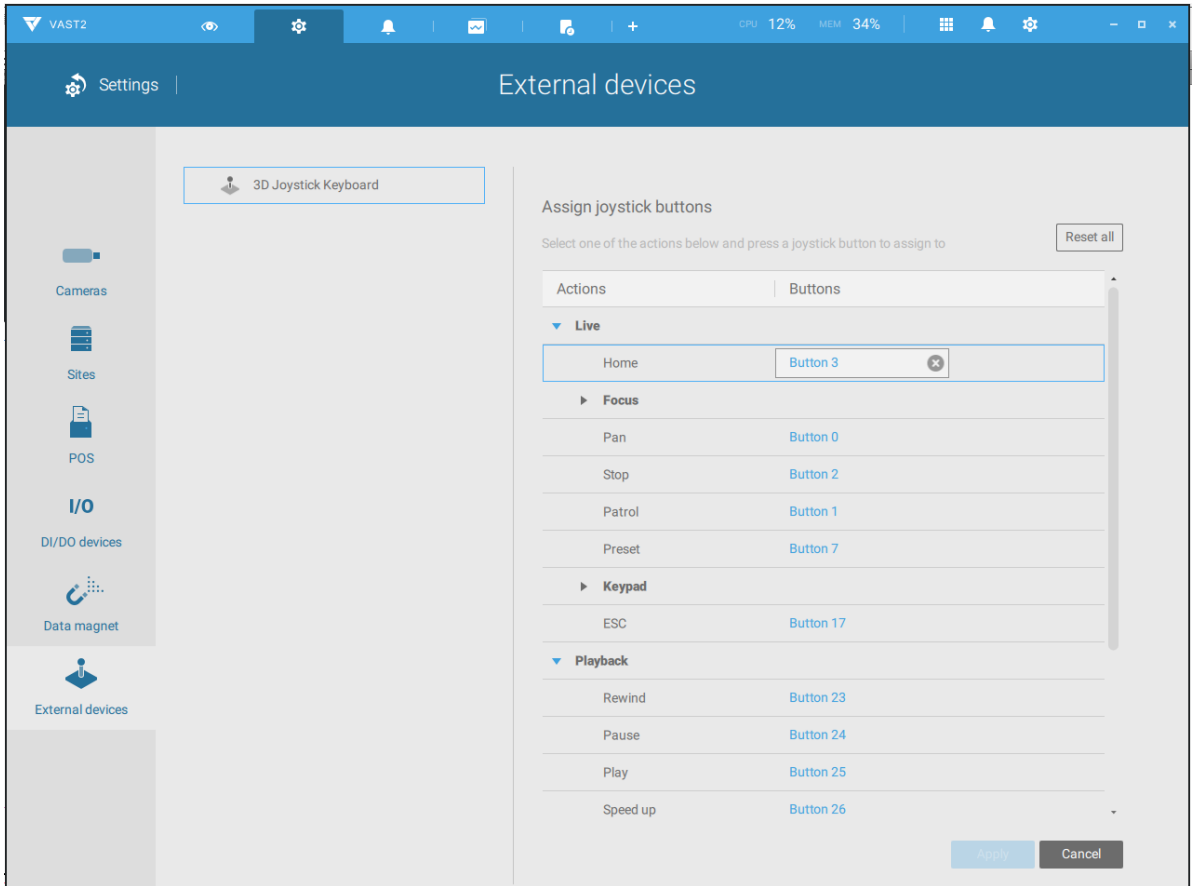
Appendix C: Joystick Support

Configurable joystick buttons

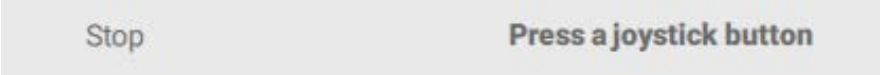
1. Connect the joystick's USB cable between the USB ports on the joystick and a VAST server/ client.
2. Once connected, you should be prompted by a connection message.



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.

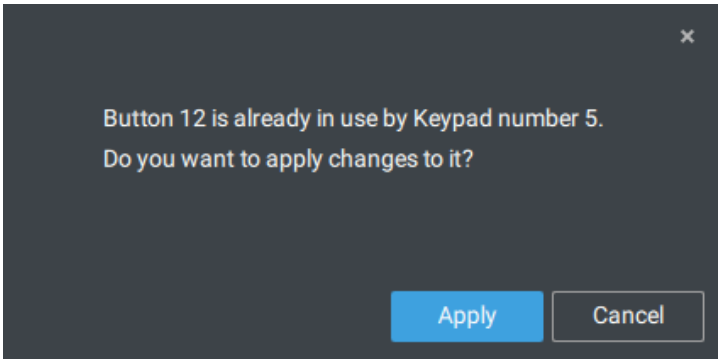


5. To assign or re-assign a button's function, single-click on the button number besides a function. Click the Delete button. The below message will display.



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.



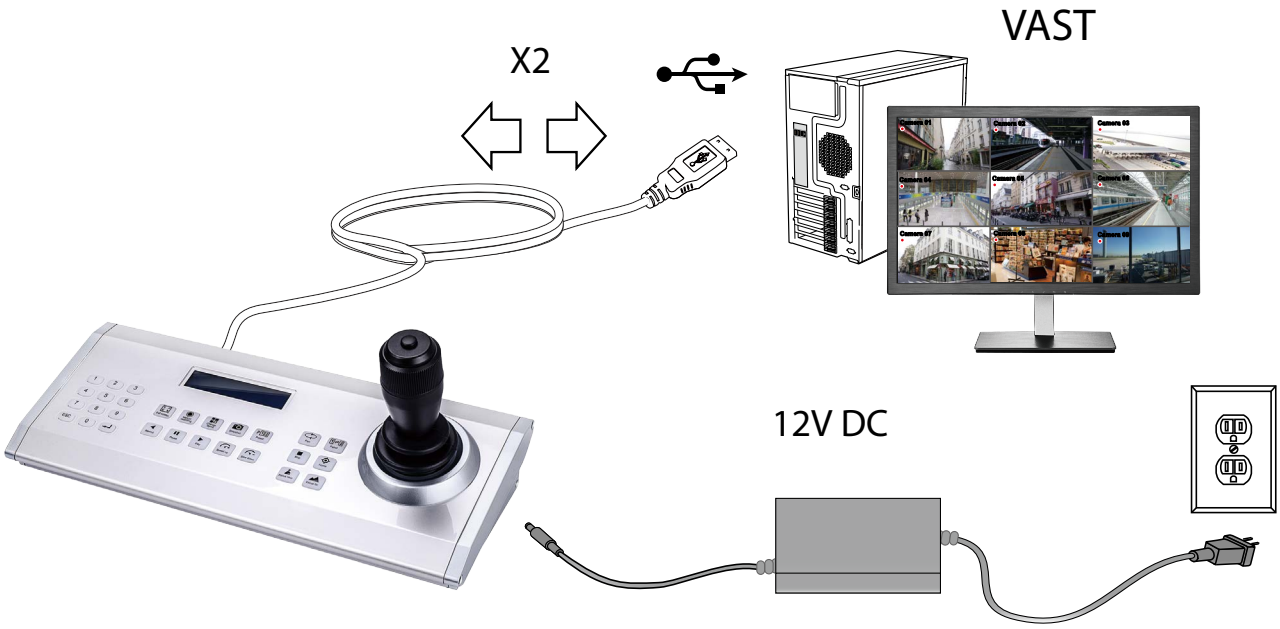
Repeat the above process and click the **Apply** button to preserve your settings.

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.

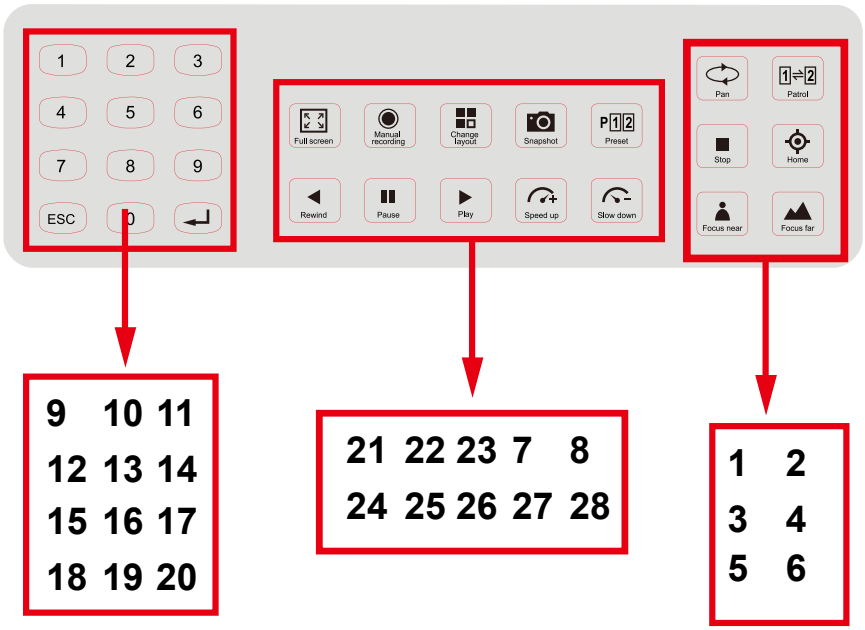


NOTE:

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 -10ºC, 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

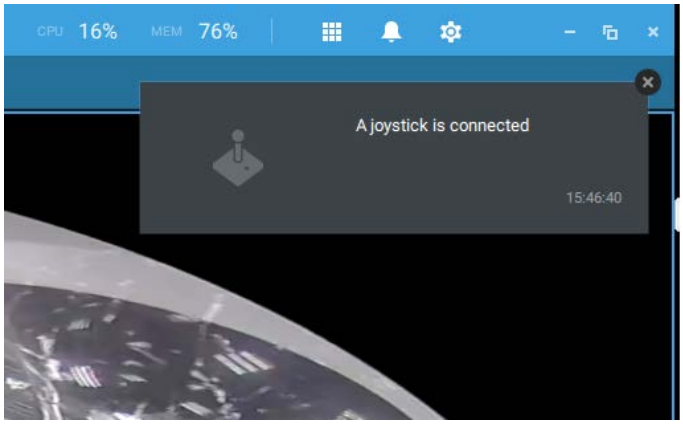
Below is the keypad numbering sequence:



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.

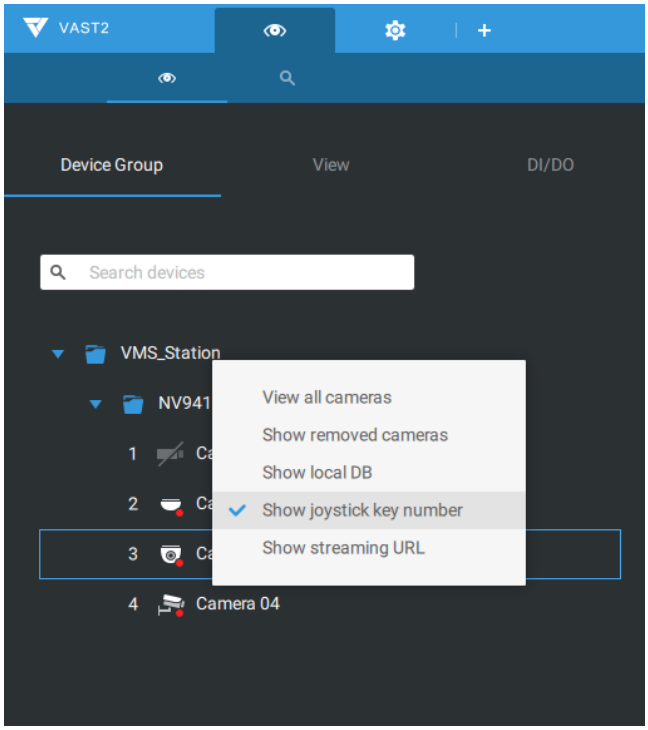


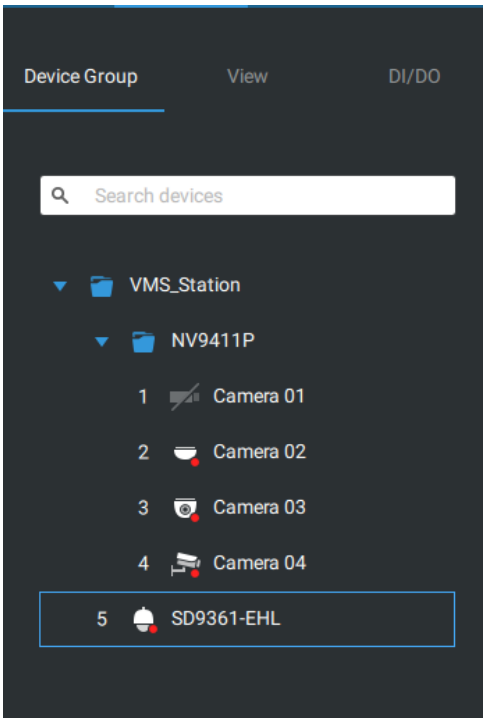
The following controls are available:

* 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 ↵, e.g., 5 + ↵. The full view of the selected camera will display.





Press the ESC key to leave the full view.

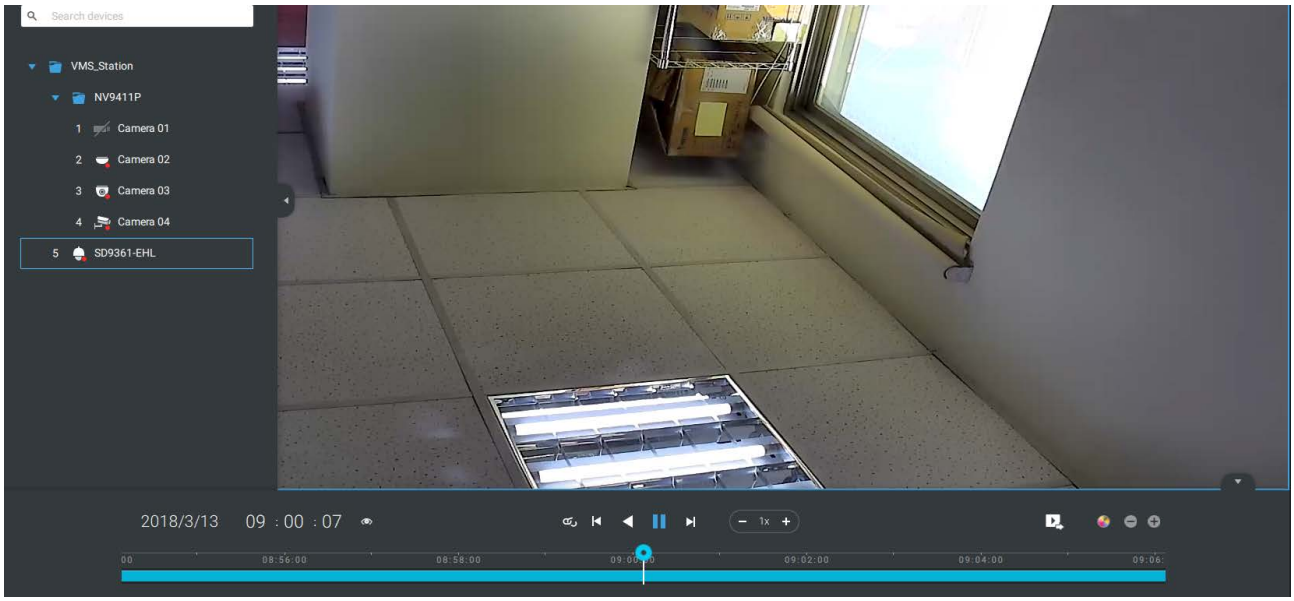
To move to a preset position, press the number key + Preset, and the Enter key ↵. The number key corresponds to the sequence number for the preset position regardless of the name of the preset.

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).

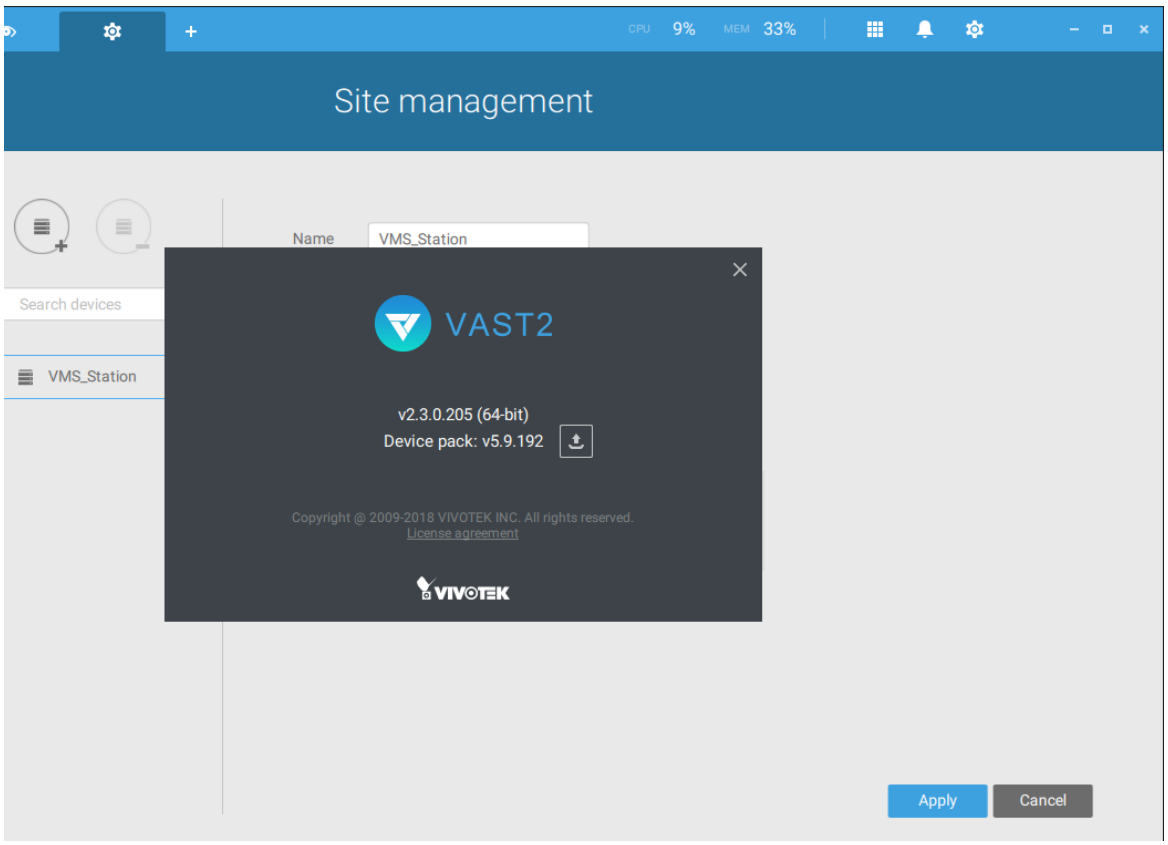
The Play button toggles the playback window. From here you can trace back the past recordings. You can use speed up, slow down, and rewind buttons here. Once the Playback mode is toggled, the point-in-time defaults to the start of the current hour.



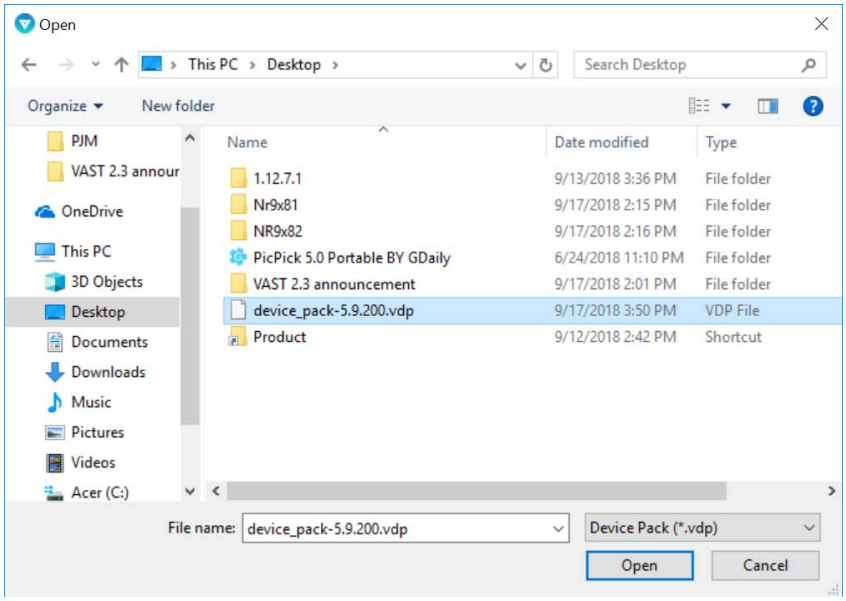
Appendix D: Upload Device Pack

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.



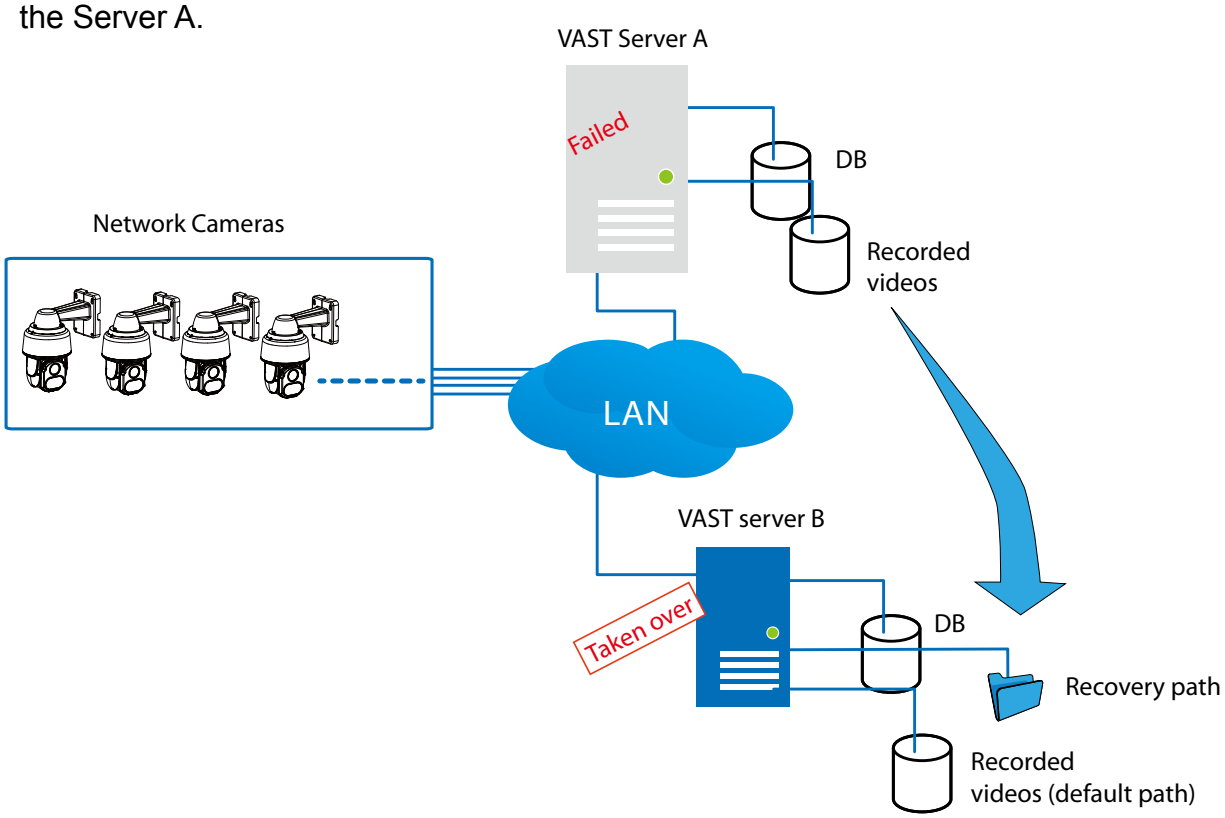
A device pack file looks like the following.



Appendix E Database Merge Function

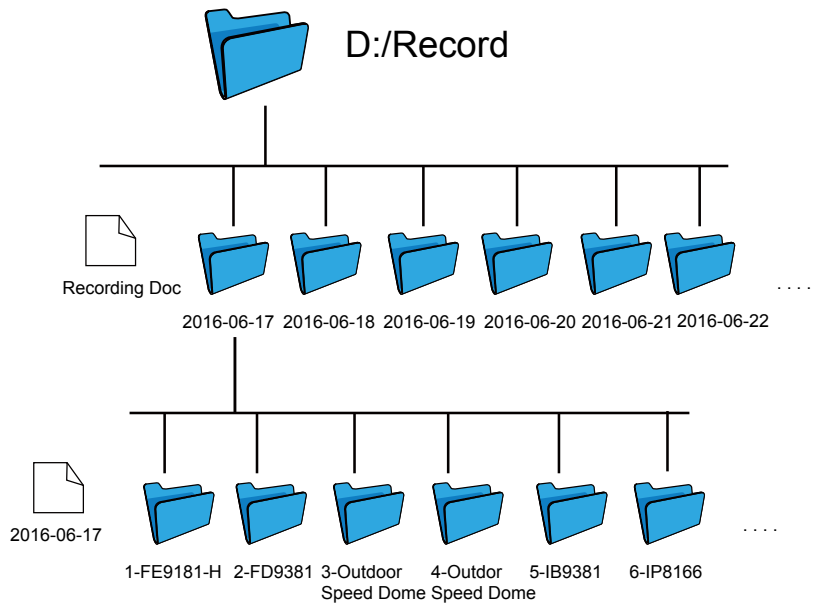
The Database Merge function applies in the following scenario:

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.

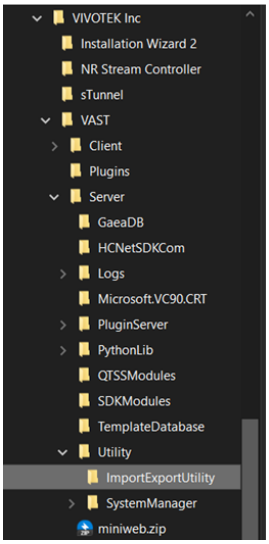


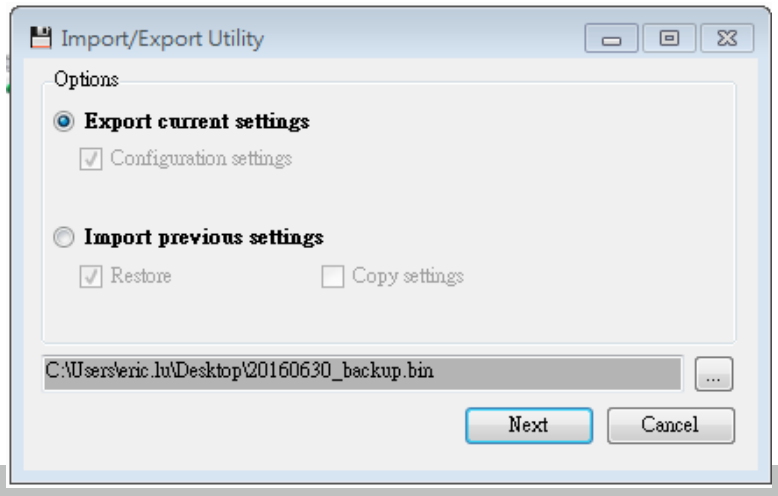
2. The VAST server B is used to continue video recording. The previous recordings on server A can be retrieved by attaching the hard disk(s) to server B or manually copying to a storage device on server B. You can then designate the location of these files as the "Recovery path" from server B. An administrator 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.



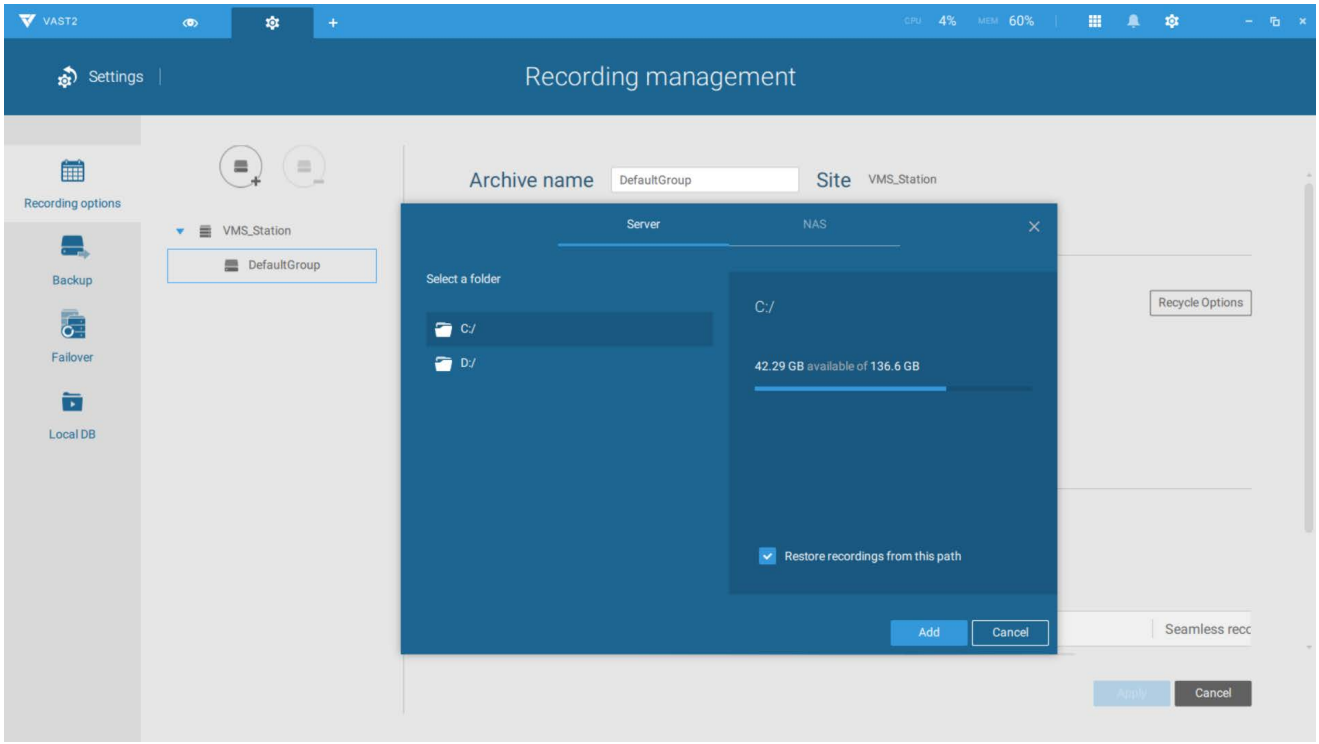
- It is also a good habit to export and preserve your VAST system configuration to prevent losses in the event of system failure. In case you want to migrate or upgrade your VAST server, you can use the Import-Export utility to duplicate your VAST configuration to another server. Copy the configuration 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**.



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:

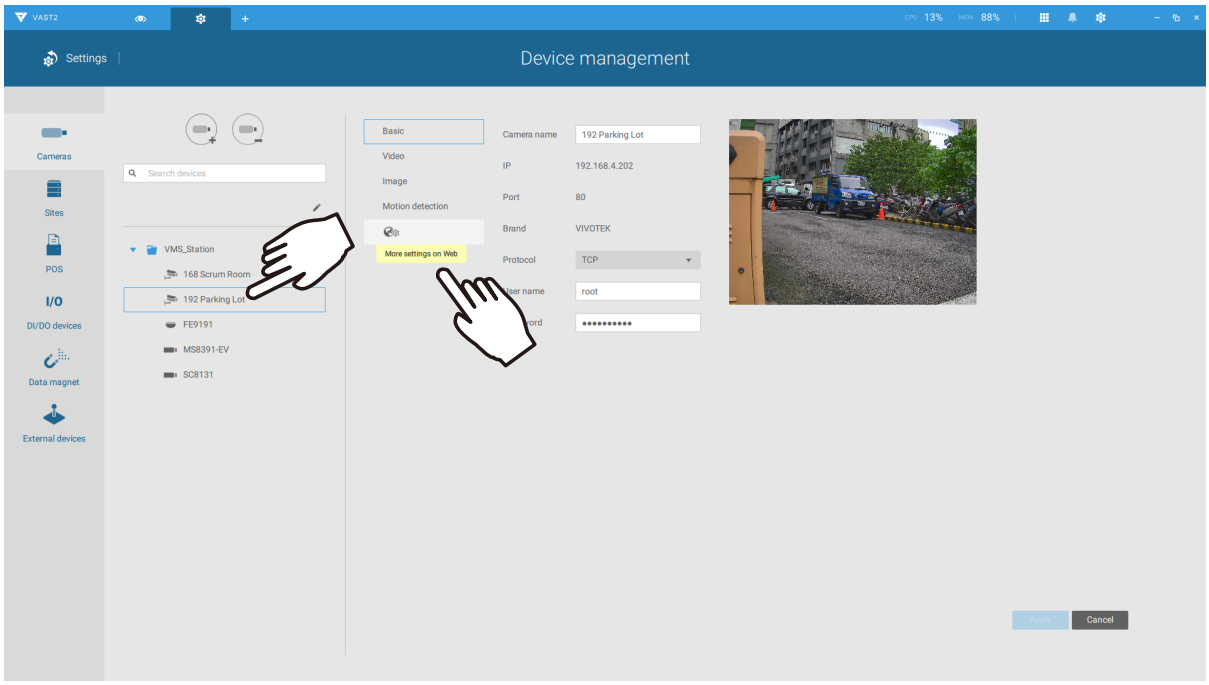
   A Local DB sub-folder will appear on the device tree. Click to select the cameras in the sub-folder to access the past recordings. The recordings in the Local DB is only accessible from the computer which has a copy of the Local DB.

For system backup options, refer to page 196.

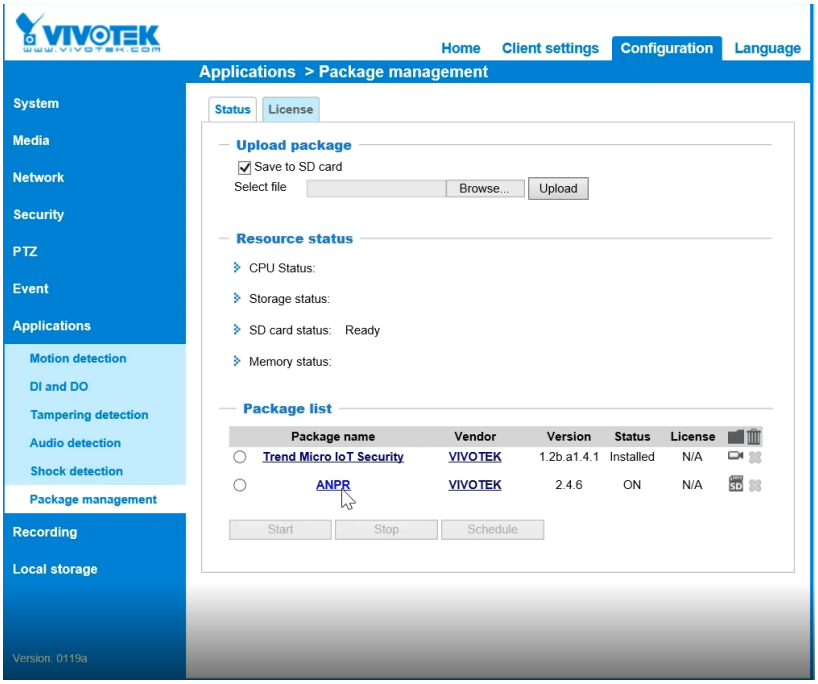
Appendix F: Using LPR Related Functions w/ Data Magnet

Acquiring data sources from 3rd-party software:

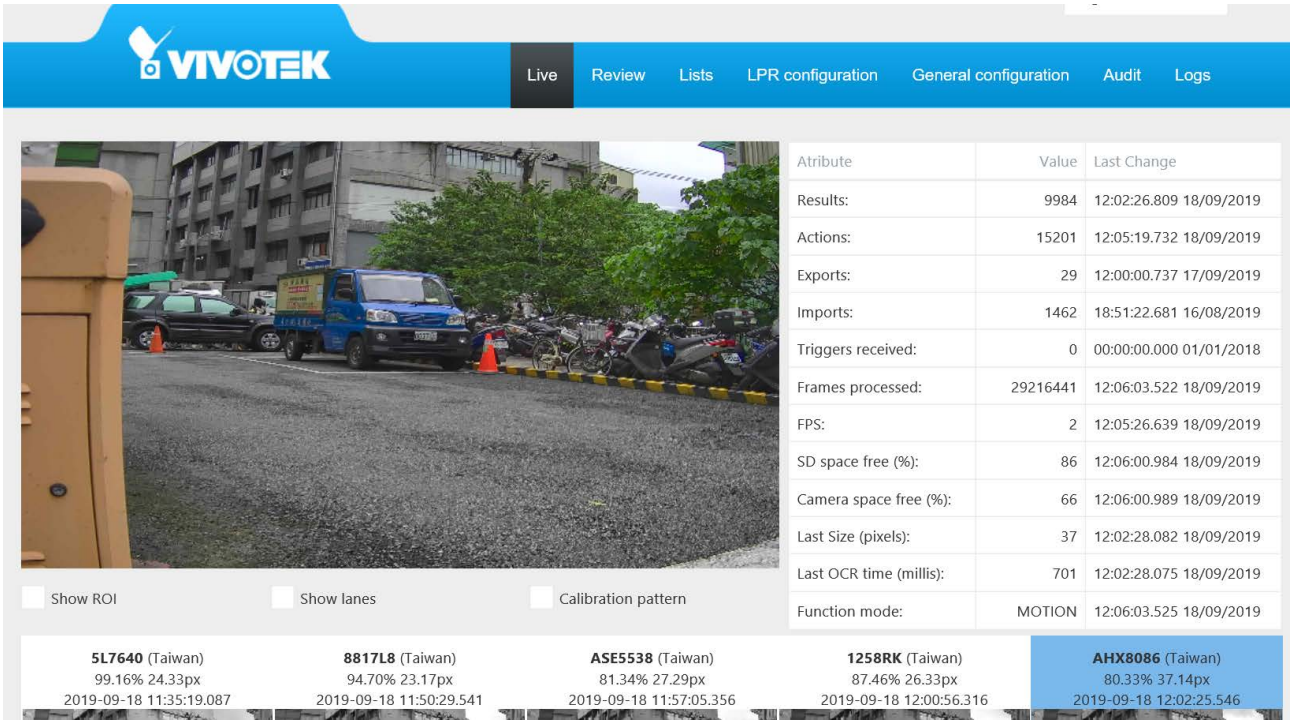
1. Select a camera that comes with the LPR (License Plate Recognition) functionality, e.g., IB9387-LPR as shown below. Click "More settings on Web" to open a web console to the camera.



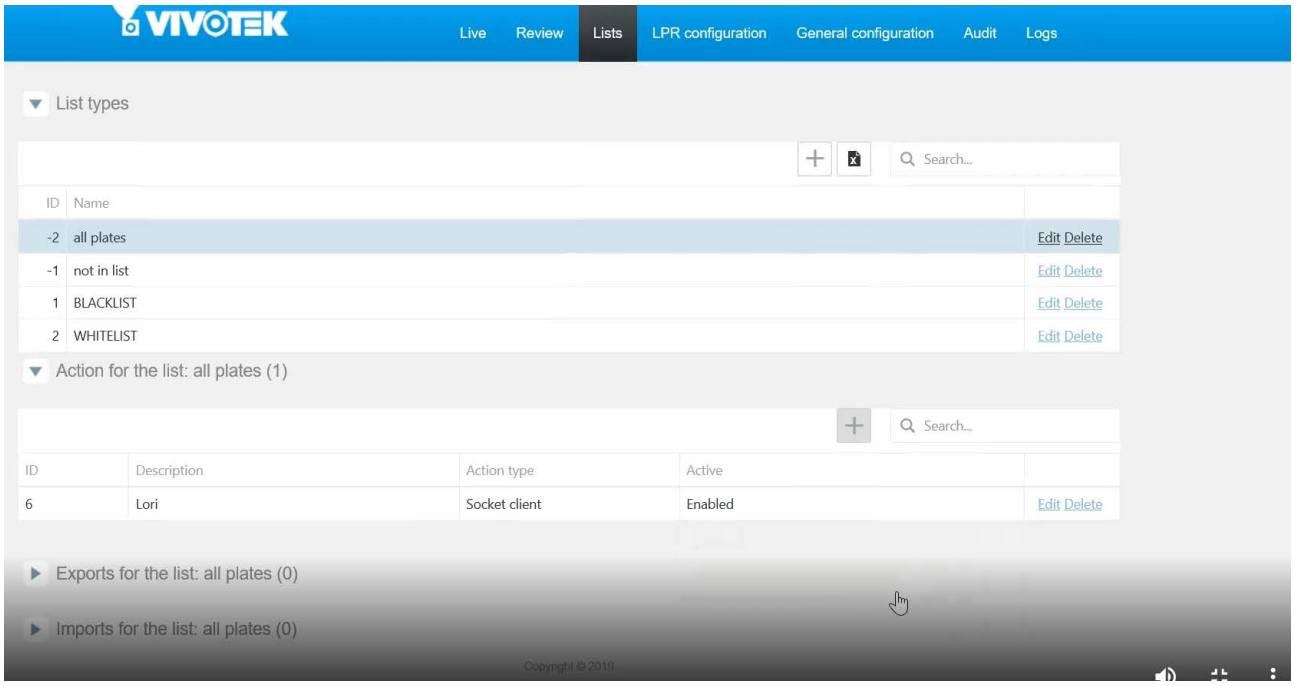
2. On the web console, enter **Configuration** > **Applications** > **Package managemen**t. Click on ANPR to open a web console to the license plate recognition software.



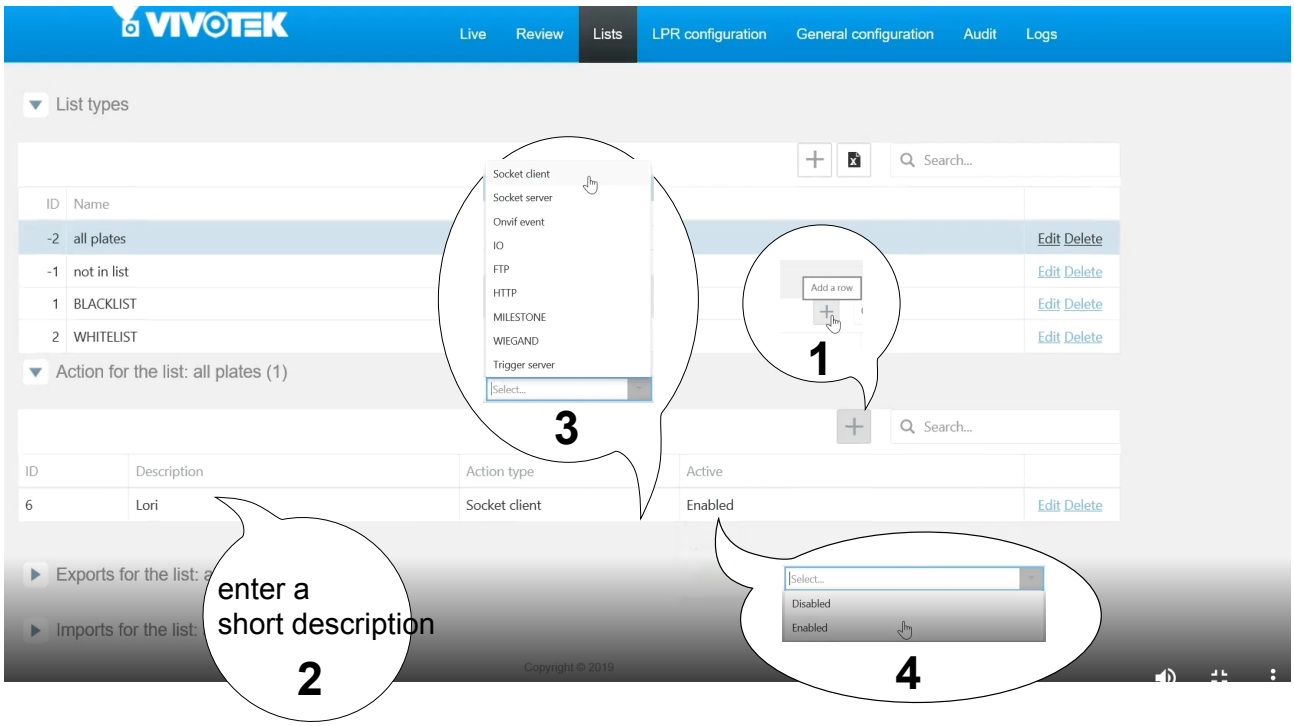
3. Click on the **Lists** tab.



4. Select a list whose data will be transmitted to the VAST server.



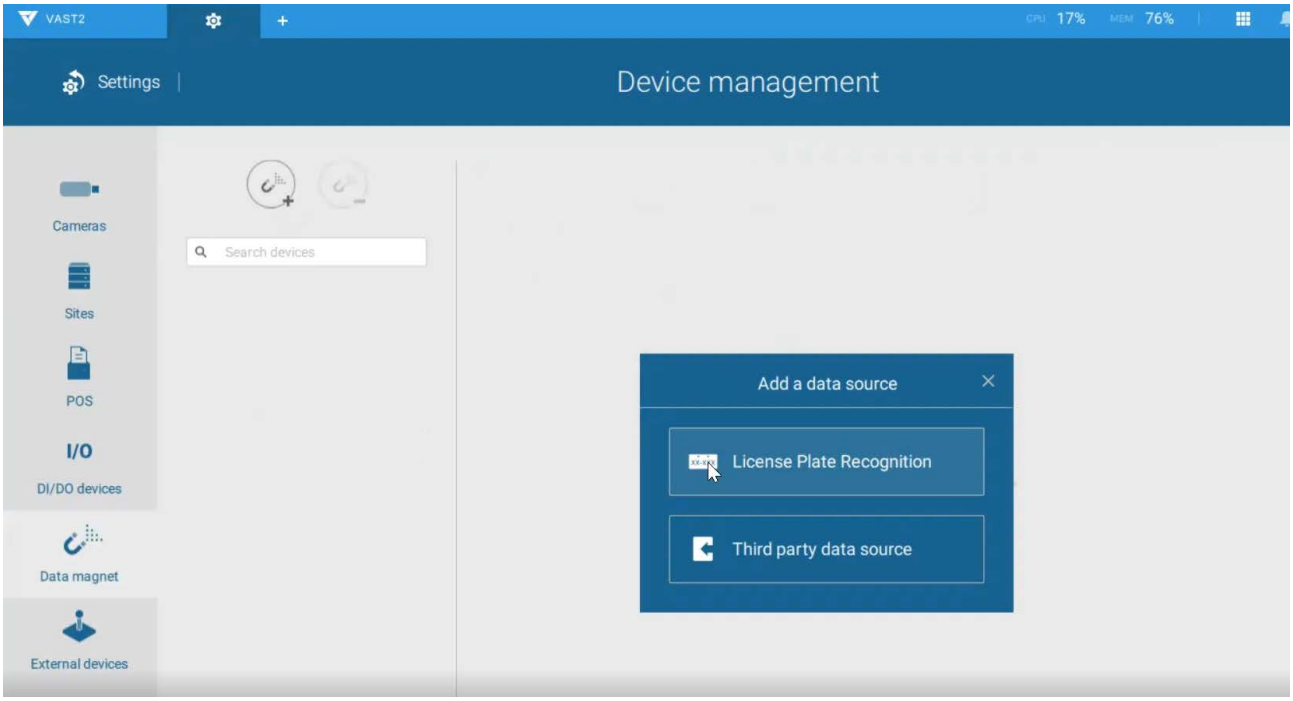
5. 5-1. Find the "Action for the list" pane. Click the "**+**" **Add a row** button.
   5-2. Enter a short description for the row.
   5-3. Select "**Socket client**" as the action type.
   5-4. Click to select **Enabled**.
   5-5. Click the **Save** button.



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.

7. 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.

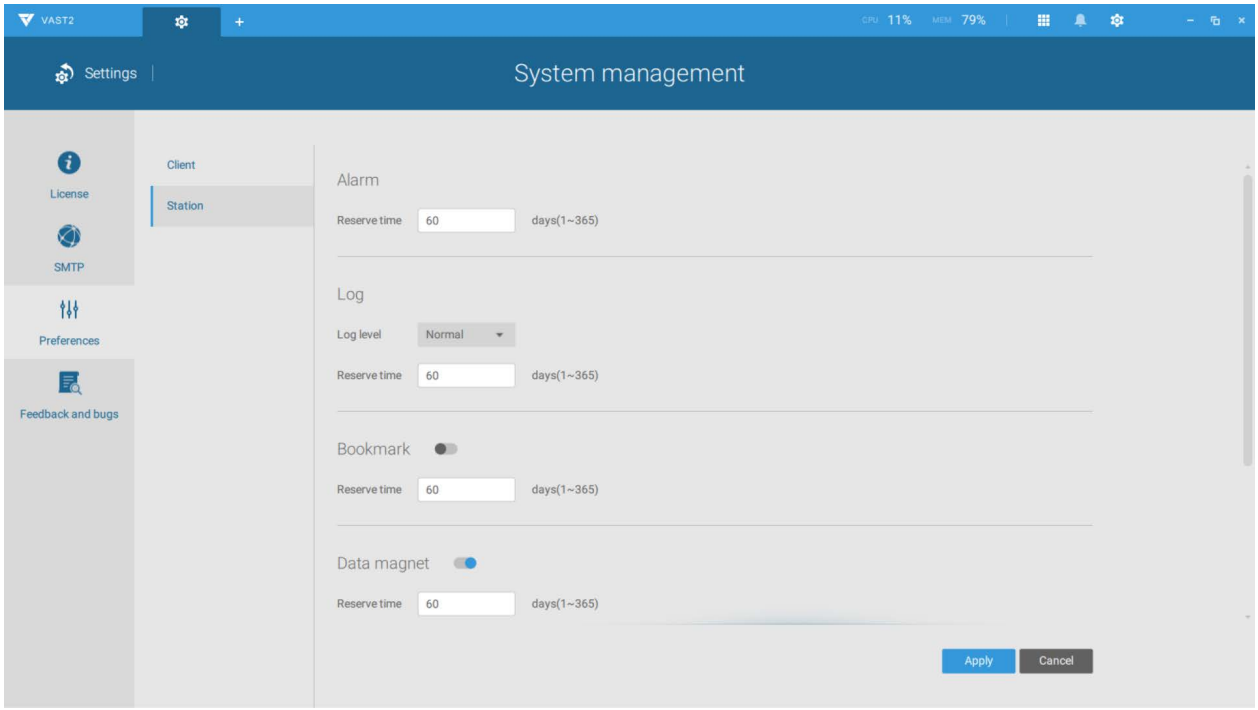


NOTE:

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.

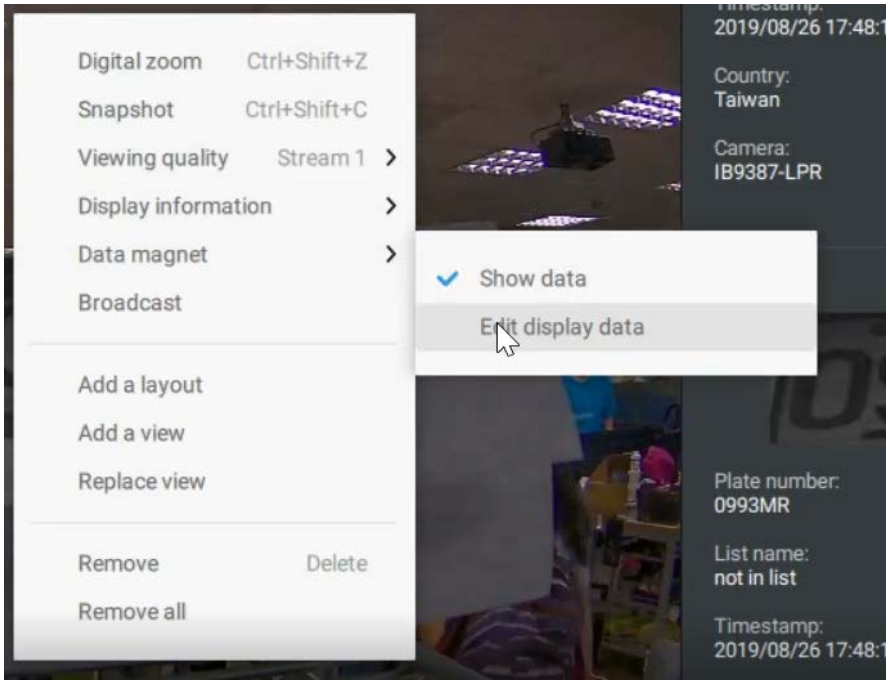
   If you need the development document for integrating 3rd-party software, please contact VIVOTEK's technical support.

   You can designate how many days the data from the data sources is retained on server in **Settings** > **System management** > **Preferences**.

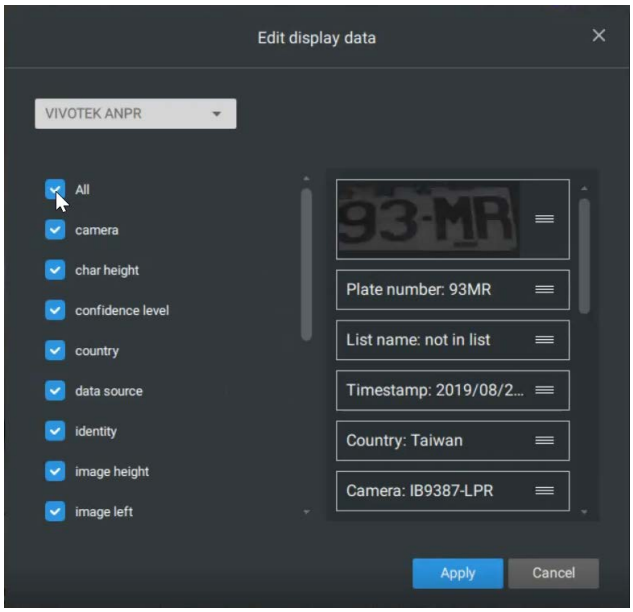


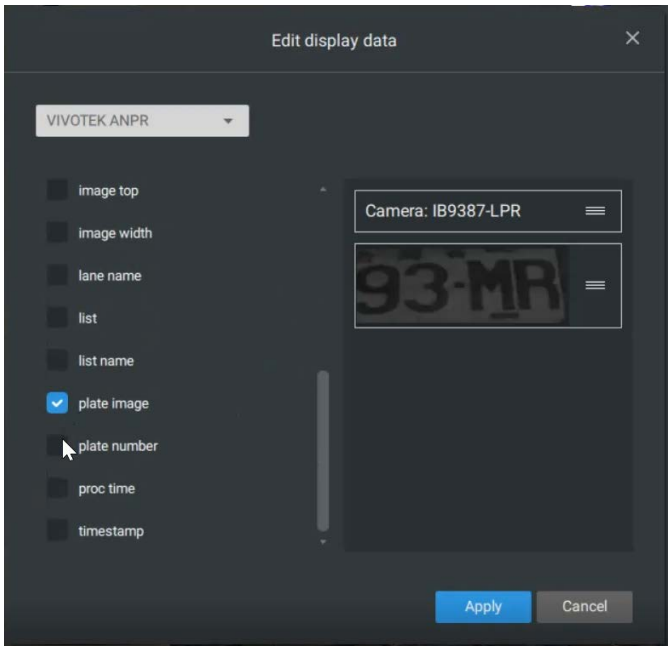
Selecting data display options:

1. On the VAST live view, right-click on screen to display Data Magnet > Edit display data.

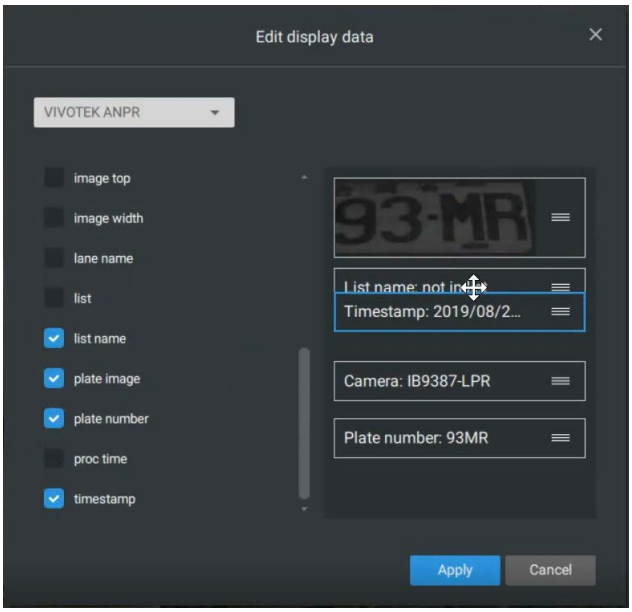


2. On the Edit pane, select all or manually select multiple display elements.



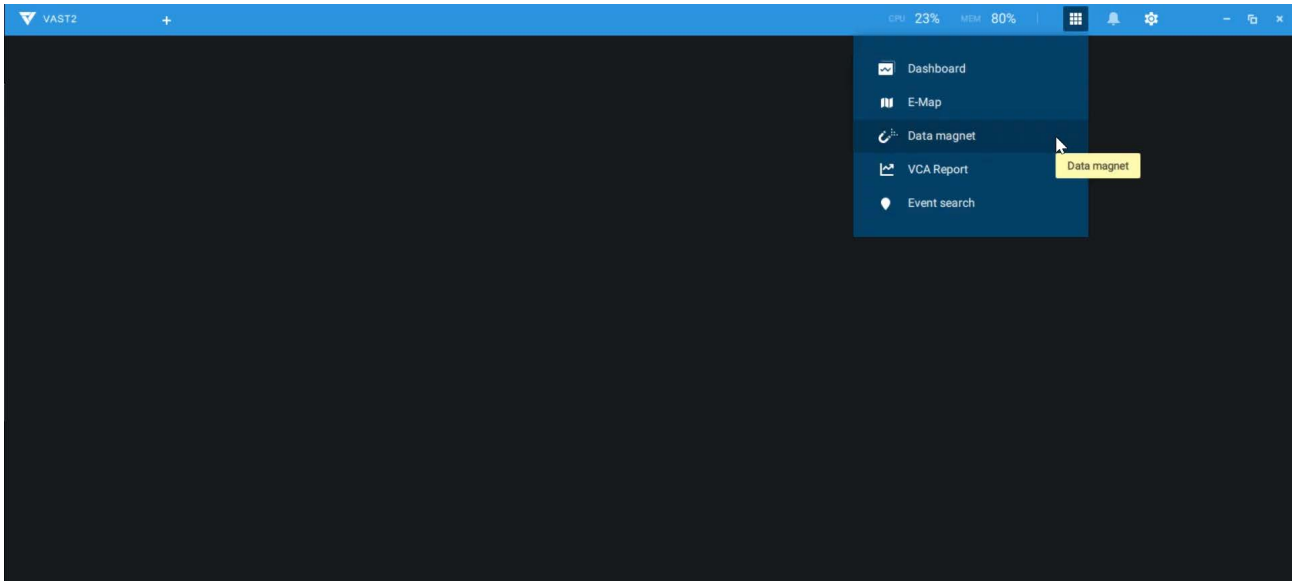


3. Click and drag individual elements to change their top-down positions on the screen. When done, click the **Apply** button.

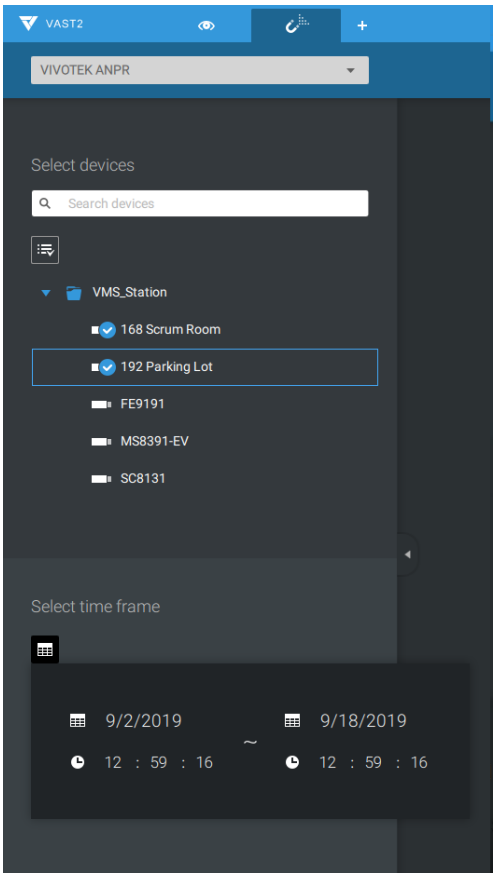


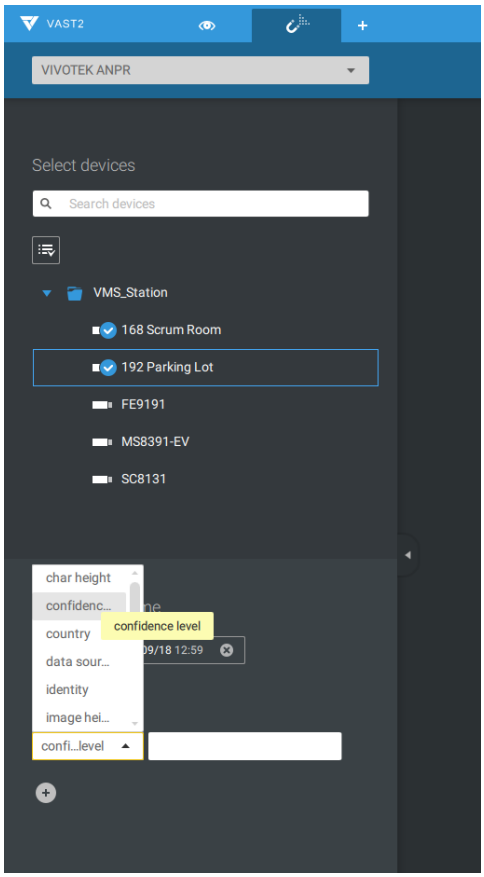
Searching for data and linked recordings:

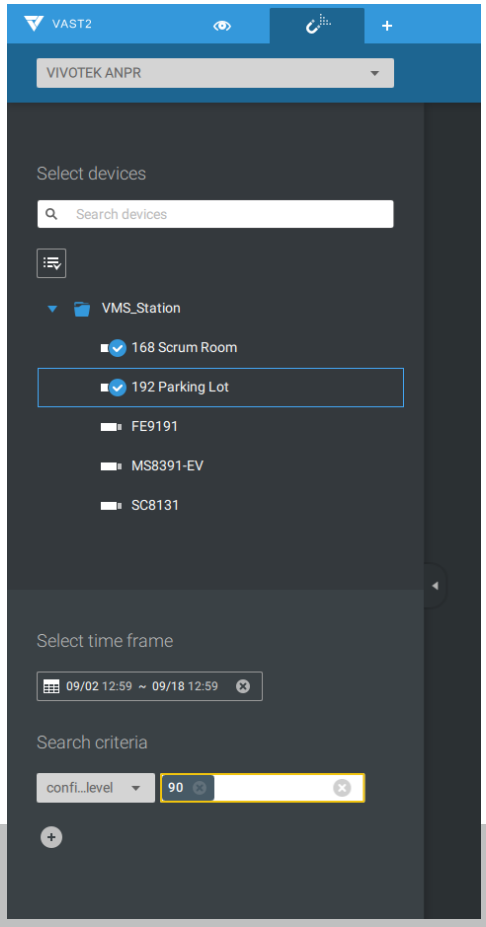
1. On the VAST live view, click on the Applications tab.



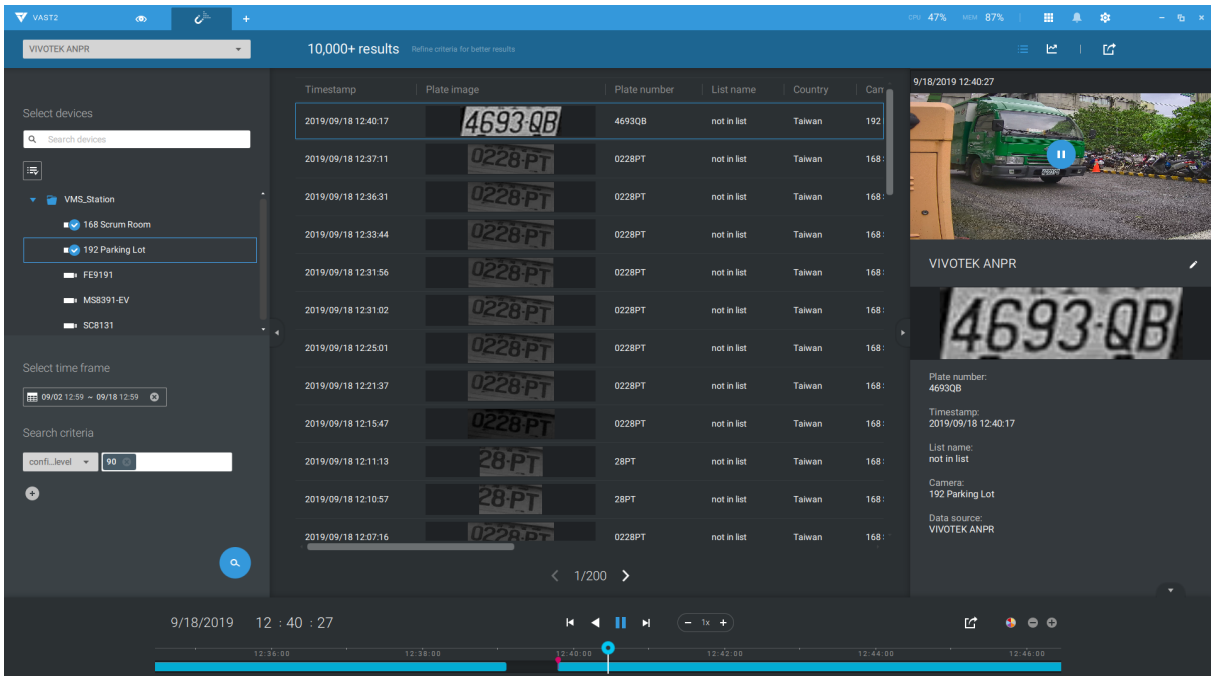
2. On the Data Magnet window, select the LPR camera, and then begin with configuring the search conditions. Select the time span from the calendar. Select to display character height, country, data source, identity, image height, lane name, list name, or enter a plate number. You can select multiple filtering conditions.



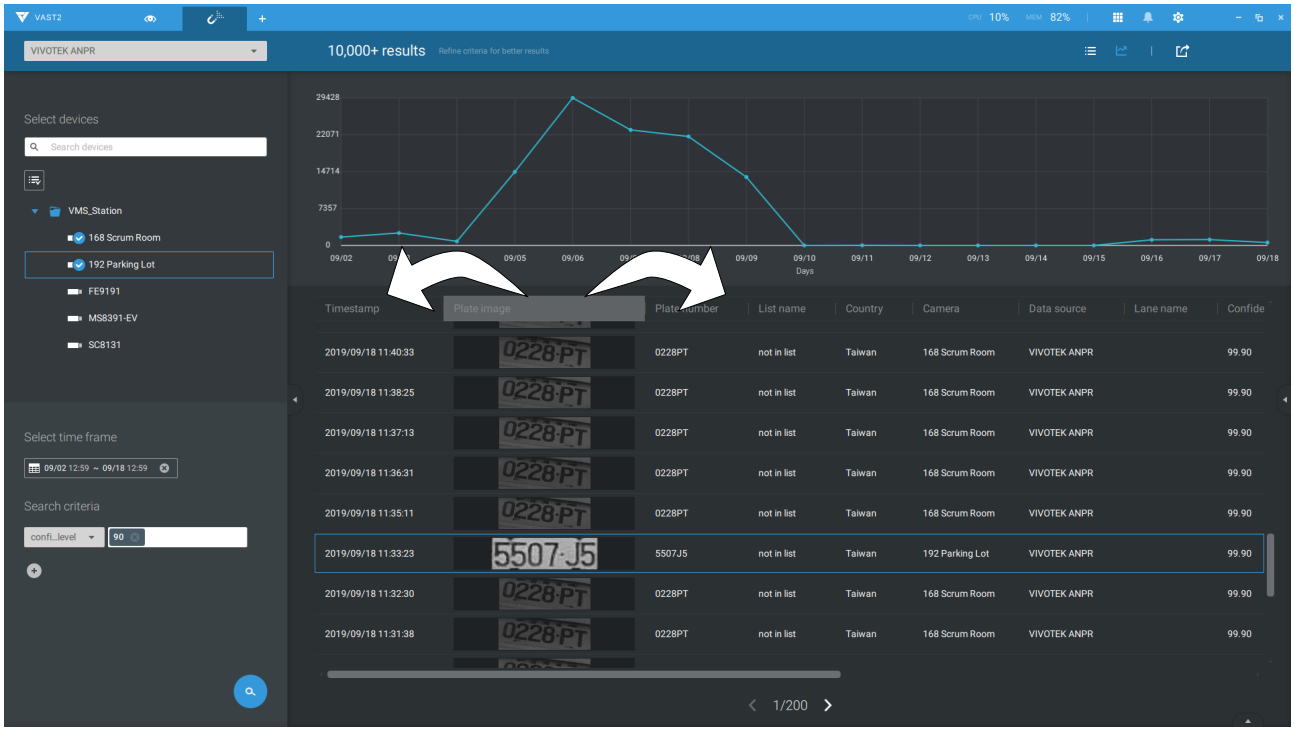




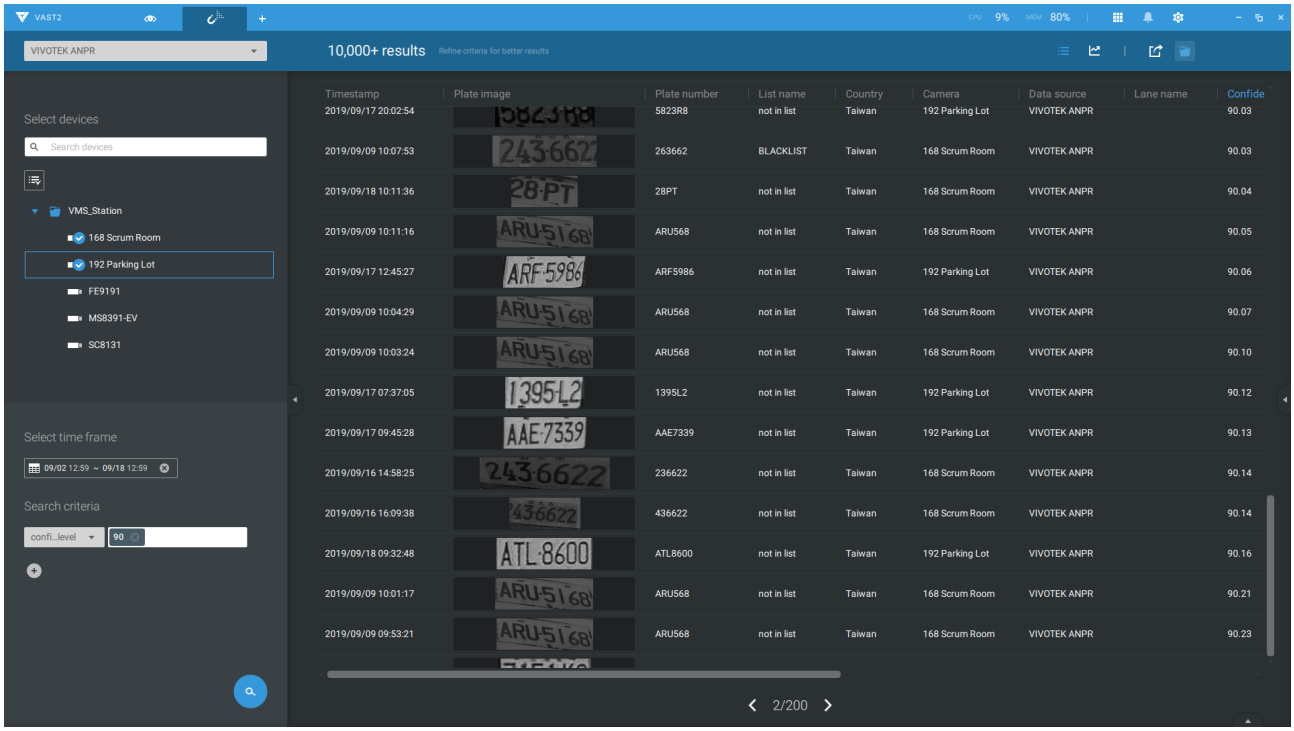
3. Click the Search button. The search results will display. Single-click to display the related video. You can also review the video in a full-screen mode.



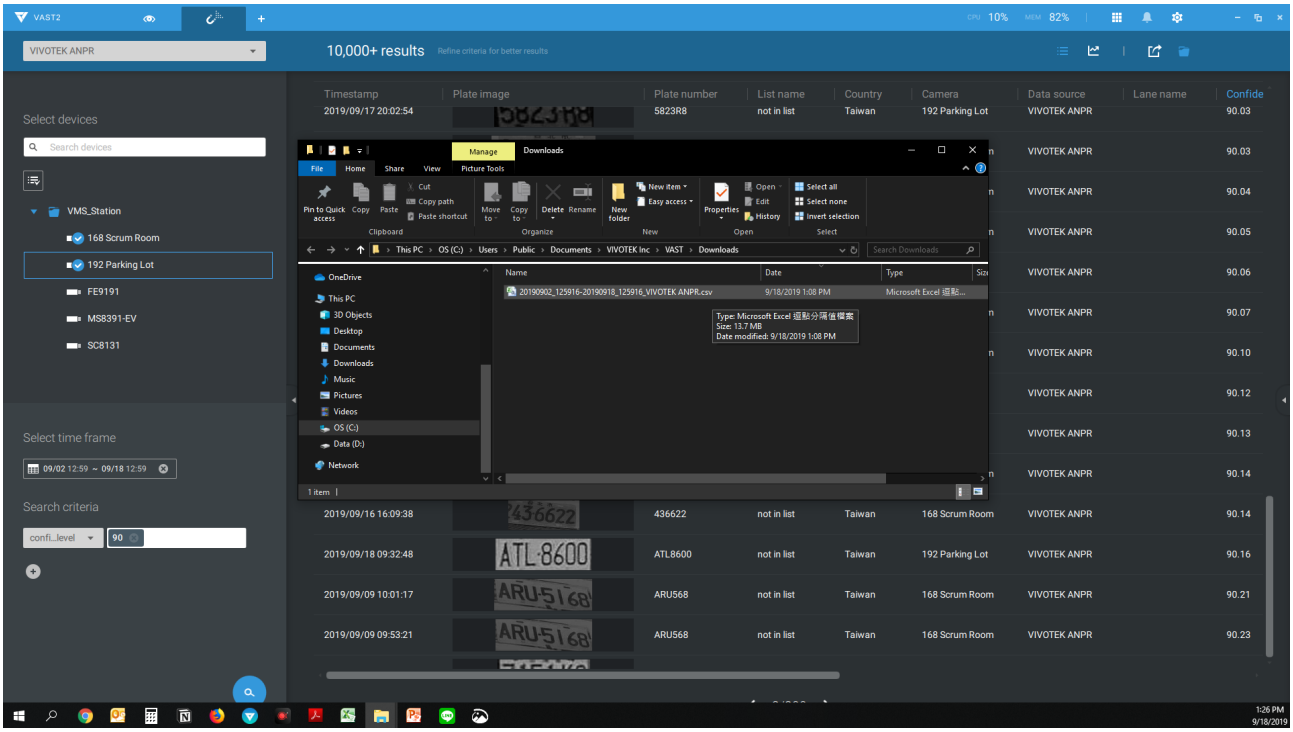
You can click and drag the display names of individual columns to switch their positions on the screen. The changes to layout are stored on the client computer. After you re-arrange the order of columns in search results, the display order will also be applied to the exported CSV file.



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.



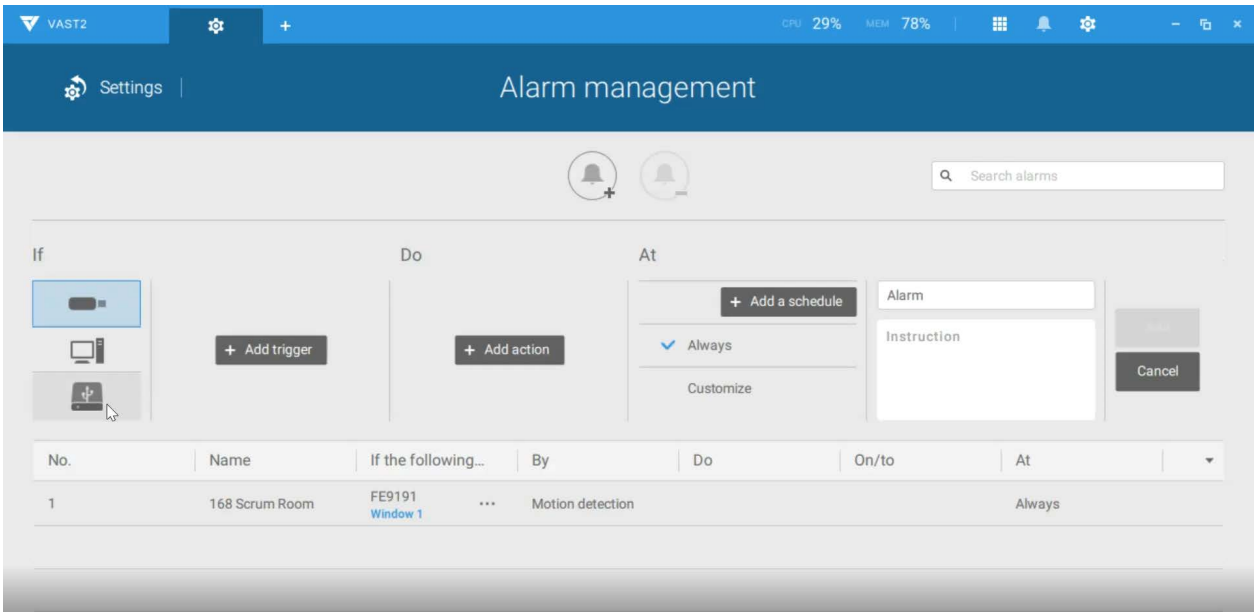
The target directory will open. Open the exported CSV file to view the search results.



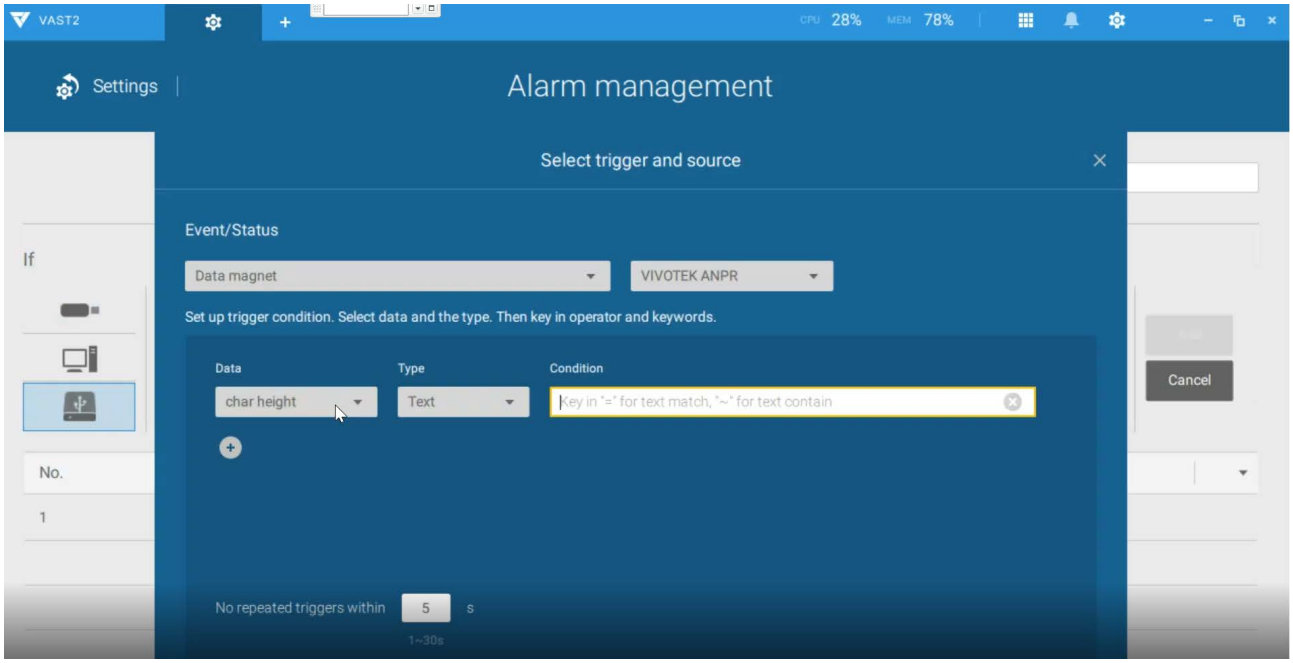
You can also open a chart view by clicking the  Chart view button. The chart view can also be exported as a png file.

Configuring Data Magnet alarms:

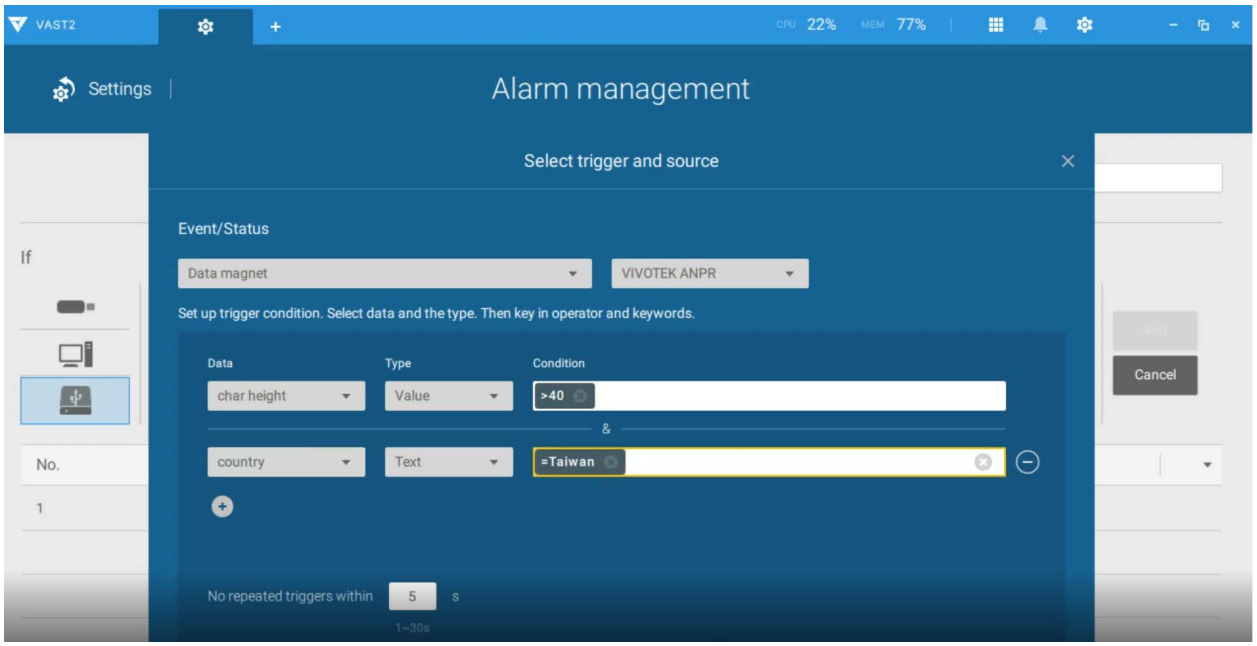
1. Enter **Settings** > **Alarm** > **Add & Delete** to create a new alarm setting. Click to select External devices.



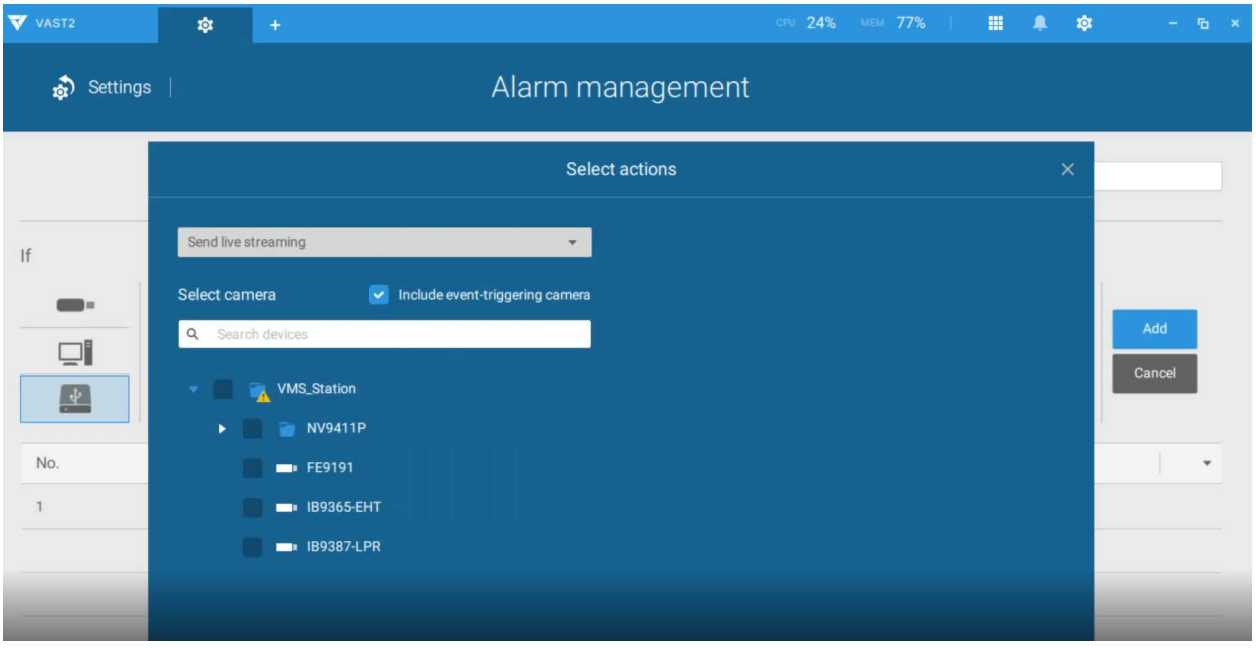
2. Select **VIVOTEK ANPR** as your triggering source. Select and create triggering conditions such as character height, image width, list, list name, country, etc. Use "=" for text matching, "~" for text containing, or approximately matching specific characters, and also ">," "<," ">=," "<=" for numbers larger or smaller than a preset value.



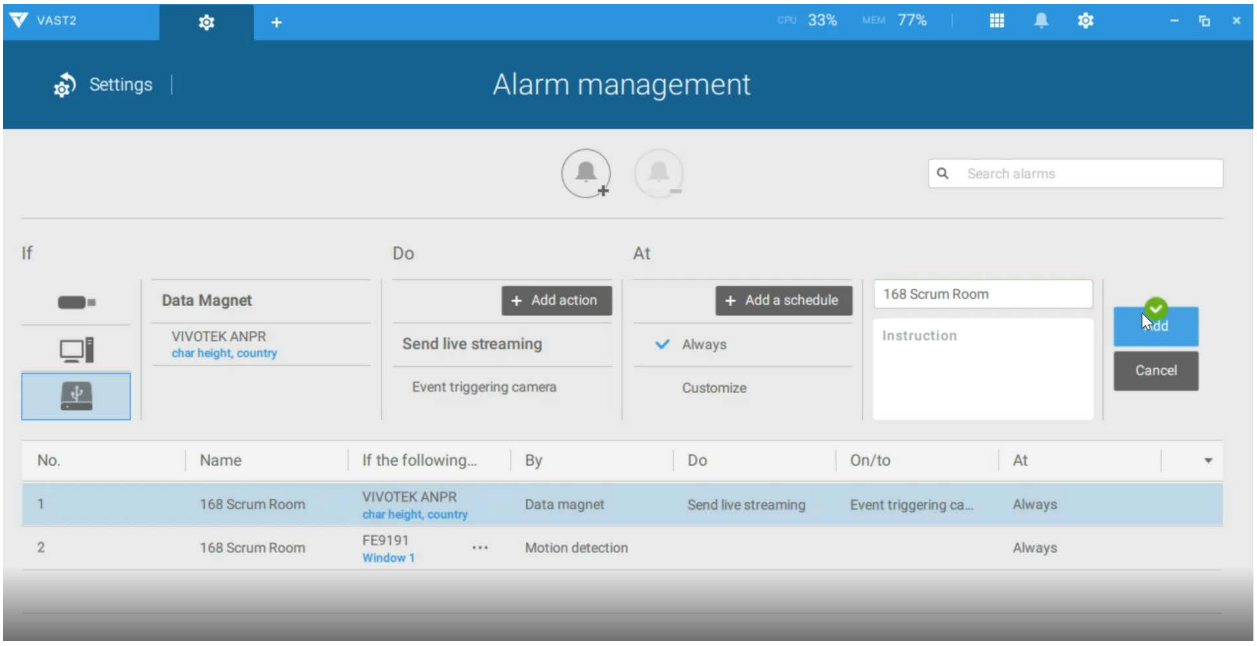
3. Continue to configure your triggering conditions. You can create multiple conditions.



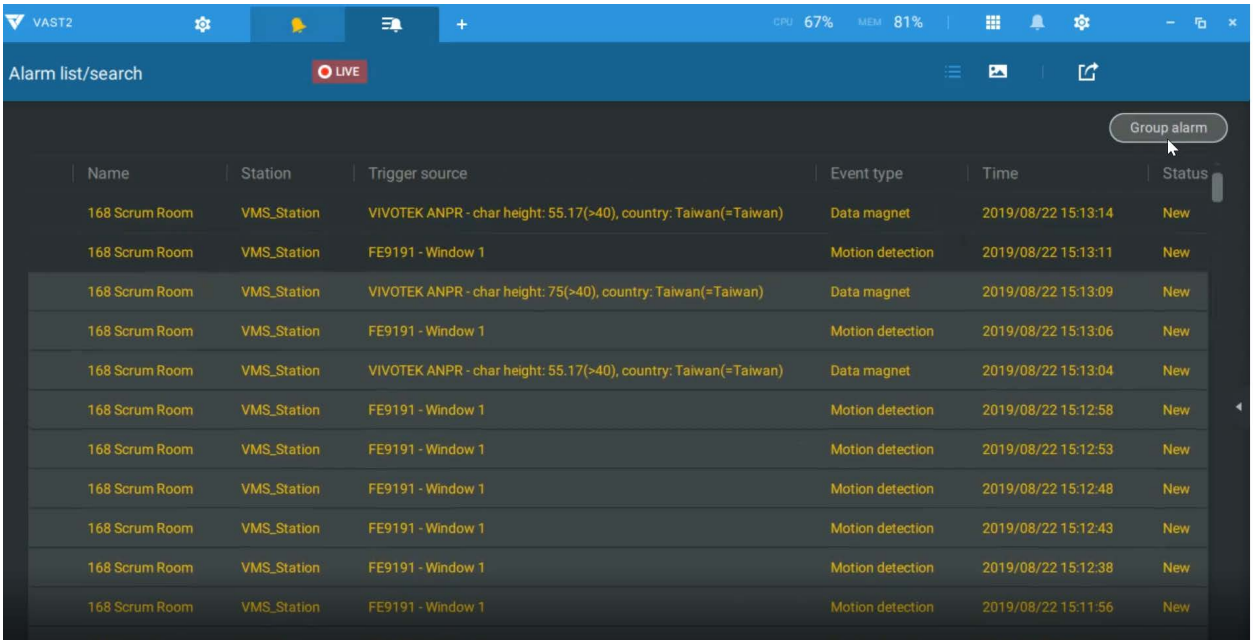
4. Continue to configure the actions for a triggered alarm, such as sending live streaming.



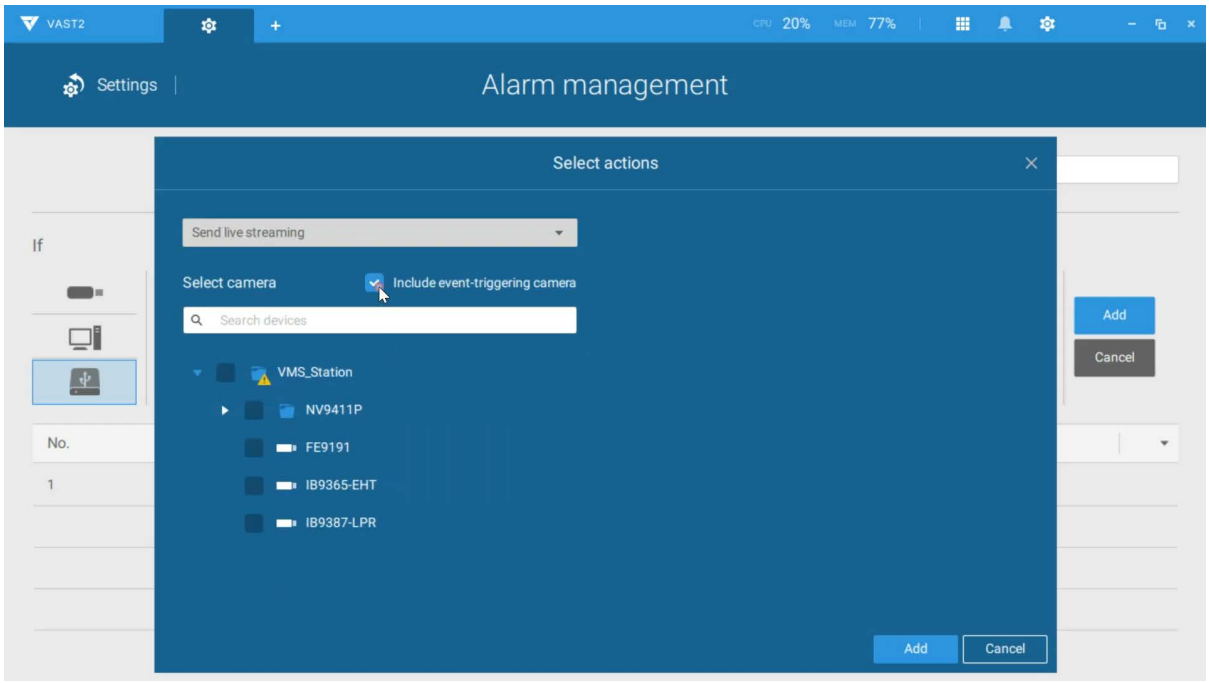
5. When done, enter a name for the alarm and click the **Add** button to complete.



6. You can now receive alarm notifications triggered by license plate recognition via the Data Magnet.

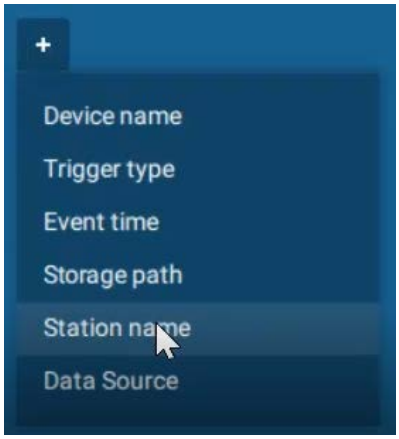


Note that if you select "Include event-triggering camera" during the alarm configuration stage, the camera delivering the data source will be automatically selected.



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.



You can specify multiple lines of information in your alarm notification message.