VIVOTEK
A Delta Group Company

VAST2

User Guide

Rev. 2.13.

For SW rev. 2.13

Contents

Revision History 5
Log in 11
Introducing VAST2 12

New Features 12

Key Features 13
Installation Option - 64-bit VAST2 Server 14
Charged Add-on Features 15
Installation Option - OpenVPN 20

Chapter 1 Basics: 23

Control and Elements 23
Live view 23
Search Pane 24
Playback Control 24
Top Tool Bar 24
View cell control 25
Text overlay 25

Hot Keys 41

View Cell Elements 44

VAST Server and Client Components 47
Multiple Server Applications 48

Minimum System Requirements 49

Chapter 2 Starting Up 51

2-1. Selecting Devices 52

2-2. Recording Options 53

2-3. Storage 64

2-4. Starting Up - Main Page 65

2-5. Saving a View 68

2-6. Add More Live Views 69

2-7. Save Your Preferences 70

2-8. Customizable Layout 71

2-9. Dashboard 73

2-10. E-Map 75
Placing DI/DO Devices 78
Configuring GIS or Google Map and GPS 79

2-11. Event Search 85

2-12. PTZ Control 88

2-13. Playback 90

2-14. Alarm 98

2-15. Search Panel 114

2-16. Smart search 117

2-17. Tour 127

2-18. Thumbnail search 129

Chapter 3 Applications: 131

3-1. I/O DI/DO Devices 131

IO Box and Related Configuration 131

Configuring I/O Box DI/DO as a Trigger or Action in Alarm 133

3-2. Configuring Redundant Servers - Failover 137

Failover Configuration Process 144

3-3. VCA (Video Content Analysis) 148

Prerequisites: 148

3-4. VAST Software License 161

Updating Licenses for VAST on Virtual Machines 169

Reminders for VAST Software License 175

Chapter 4 Settings: 176

4-1. Settings > System > Preferences 176

4-2. Settings > Device > Cameras 183

4-3. Logical Folders 186

4-4. Settings > Recording > Recording Options 189

4-5. Settings > Recording > Backup 191

Storage 194

4-6. Settings > Device > Stations 195

Multicasting 198

4-7. Settings > Device > External Devices > POS 202

4-8. Settings > Device > Local DB 203

4-9. Settings > System > SMTP 207

4-10. Settings > IO Box and Related Configuration . 207

4-11. Settings > User Management 208

4-12. Settings > VIVOCloud 212

Appendix A: VAST Service Control Tool 216

Appendix B: Fisheye Camera Dewarp Modes 217

Appendix C: Matrix 224

Appendix D: Joystick Support 229

Appendix E: Network Audio Solution 235

Appendix F: Upload Device Pack 240

Appendix G: Using LPR Related Functions w/ Data Magnet 242

Appendix H: Enable Smart Tracking for Speed Dome Cameras 265

Appendix I: Multi-factor Authentication for Access Control 266

Revision History

Rev. 1.0:

* Initial release.

Rev. 1.1:

* Added DI/DO devices display on E-Map.
* Added the support for GPS-enbaled vehicle on Google Map.
* VCA report now supports a cross-day format
* Added Two Way Audio on camera view cell control.

Rev. 1.2: (July, 2017)

* Added the description for the Backup related function.
* Added the description for the Redundant server (Failover) functions.
* Modified the User section for allowing Windows AD users.
* Modified the description for some screen elements, such as the removal of the Replay function, and the change of Playback tab from top tool bar to the individual camera view cell, etc.
* Added the description for the Google map and GPS implementation.
* Added the Windows Active Directory integration in User Management.

Rev. 1.3: (Nov., 2017)

* Added the description for the Go to E-Map option in Alarm setting.
* Added the information for updating MAC licenses for VAST on virtual machines.
* Modified the VAST architecture drawing. Added information for adding an NVR in a VAST configuration.
* Modified the description for camera password authentication.
* Added Streaming URL as an optional method to add camera.

Rev. 1.4: (Nov., 2017)

* Minor corrections for software rev. 5700.

Rev. 1.5: (Mar., 2018), software rev. 6647

* Implementations for mobile NVR:

- management access	- VAST2 installation with VPN
- Live monitoring with GPS locations.	- Query GPS path
- Emap with GPS information	- Camera live view on Google map
- Mount local database: read GPS data or recordings from external USB devices	
- Receives alarms from mobile NVR.	

* Mount local database: (see page 203)
  - Reading GPS data or recordings from external devices (USB).
  - Mount scheduled backup recordings from VAST scheduled backup videos.

* VCA report supports customizable report intervals for CSV data.
* Supports ONVIF camera event recordings.
* Supports fisheye Regional view auto pan function.
* Smart search function applicable to the recordings on the NR and ND series NVRs.
* Supports VCA alarm prompts from Crowd detection and Smart Motion detection.
* Supports installation with OpenVPN server. NAT-traversal connection with mobile NVR.
* Bookmarked clips are exempted from storage recycles. See page 91.
* Joystick support. See page 228.
* Log search is available with this release.

Rev. 1.6: (June, 2018), software rev. 7970

* Supports Matrix client. See Appendix C on page 224.

Rev. 1.7: (June, 2018), software rev. 8222

* Supports Log management. See page 27.
* Supports Alarm list. See page 34.
* Supports Alarm Acknowledgement
* Updated Hot keys.

Rev. 2.2: (July, 2018), software rev. 8222

* Coordinated document rev. no. with that of the software major release.

Rev. 2.3: (Sept., 2018), software rev. 2.3.0.205

System Settings:	
	* Added new User privilege options for operation, configuration, and accessible devices. See page 208.
	* Added and consolidated Top tool bar to implement related functions.
	* VAST server port configurable in Settings > Device > Stations.
	* Added the Import Device Pack function. See Appendix E at page 240.
	* Alarm/log preservation time configurable. See page 176.
	* NTP server configurable to be listening to a user-supplied NTP server. By default, VAST synchronizes camera's time with its time. See page 185.
Alarm Management:	
	* Supports MOXA I/O box.
Integration:	
	* Supports speed dome wiper blade operation.
Enhancements:	
	* Supports dewarped snapshot for fisheye cameras. See page 90.
	* Supports Google map API key. See page 79.
	* Supports Auto login to avoid repeatedly entering credentials. See page68.
	* Added event triggers to scheduled recording options. See page 54.
	* View cell text overlay display options. See page 24.
	* Dashboard for system status display. See page 73.
	* Matrix now supports views, camera tour, Dashboard, E-map, and Alarm. See page 224.

	* New installer wizard.
	* Supports configurable joystick button settings. See page 229.
	* Updated hot keys table. Hot keys combinations for Macintosh machines are also included. See page 41.

Rev. 2.4: (Dec., 2018), software rev. 2.4

	* Added new hot keys for the Alarm search pane on page 43.
	* Added the E-map in view cell feature. See page 67.
	* Updated Settings > System > Preferences options. See page 176.
	* Added VCA detection as Alarm triggers. See page 98.
	* Added the Number of Remaining People as an alarm trigger. See page 100.
	* Updated details about charged features. See page 15.
	* Updated Smart Search description. See page 117.
	* The Alarm Search window is replaced by the Alarm list accessed from the tool bar. See page 34.
	* Added the description for the Alarm tab window. See page 40.
	* Added the audible alarm configuration on page 107.
	* Added the regular VCA report option on page 118.
	* Added the description for Smart search II function on page 124.
	* Updated the calculation rules for the charged features on page 15.

Rev. 2.5: (Mar., 2019), software rev. 2.5

	* Changed TCP Message parameters. See page 104.	
		- A trigger message does not need to match all characters.
		- Provides the options for: Letter Case sensitive, the text messages containing or matching the preset text.
	* Added the Add bookmark function in the Event > Action setting. See page 67. The alarm bookmarks (recorded video clips) will not be recycled.	
	* Allows a Google map to be placed into view cells.	
	* Added Alarm thumbnail view and alarm list with editable alarm status and comments. Security personnel can evaluate the alarms and put handling statuses with the alarm occurrences.	

Rev. 2.6: (Aug., 2019), software rev. 2.6

	* Added the Group alarm function. See page 109.
	* Updated the VAST licensing feature for the installation on virtual machines. See page 169.
	* Updated the Google map related configuration. See page 84.
	* Updated the NAS (Network Attached Storage) configuration. Multiple network shares can be designated as recording paths. See page 60.
	* Added Appendix F for using 3rd-party software via the Data Magnet functionality. See page 242.

Rev. 2.7: (Feb., 2020), software rev. 2.7

	* Added description for Smart Search II Plus (Line Crossing, Loitering, Intrusion detection). See page 117.
	* Added description for Smart Tracking. See page 265.
	* Added description for Live Multicast for reduced use of network bandwidth. See page 198.
	* Added Failover server for the CMS server in a Failover configuration. This provides redundancy for the Central Management server. See page 137.
	* Highlight unusual data and data overlay on screen. See page 254
	* Added a complete list of event types on page 28.
	* Added watermark for video feeds on client computers. See page 157.

Rev. 2.8: (May., 2020), software rev. 2.8

	* Added support for Remote Focus control on view cells (for cameras that come with a zoom lens). See page 46.
	* Added a Trigger period (time span) for the DO status in the Alarm management window. Users can determine how long a DO trigger is effective. See page 105.
	* Added the support for the GIS map as an alternative to Google map in the Emap window. See page 137.
	* Added the support for Playback Data magnet display data. See page 92.

Rev. 2.9: (Aug., 2020), software rev. 2.9

	* Added the support for the limitations on user's privileges for camera audio input. Added a volume slide bar. See page 46.
	* Added a watermark password, text overprint on the recorded/exported video, and Digital watermark for Standalone player. (Previously available on Live View only). See page 179.
	* Added the support to temporarily disble all VAST2 and NVR alarms with a configurable alarm disabled time period. See page 100.

Rev. 2.10: (Jan., 2021), software rev. 2.10

	* Added Data Magnet Watch List and Rule configuration settings for black and white list access control. See page 247.
	* Provided the Evidence Images for LPR cameras in the Data Magnet. See page 259.
	* Added the support for adding a web page in view cells. See page 66.
	* Added the support for People running alarm.
	* Added System warning with lack of virtual memory. See page 177.
	* Added the support for a warning message with incongruent Client and Server software versions.
	* Added a message prompt when the Seamless recording feature cannot be used. See page 58.

Rev. 2.11: (Apr., 2021), software rev. 2.11

	* Added quick access to Data Magnet data source with a search function. System will list data magnet data happened within 24 hours. See page 252.
	* Individual VAST clients can configure what kinds of alarm notifications can be delivered to them. See page 100.
	* Added the support for NVRs added via a VIVOCloud account. See page 212.
	* Added the support for the Thumbnail search of the recordings under Linux NVRs. See page 129.
	* Added the support for skipping VAST2 display on a specific monitor. See page 177.
	* Added a note for the 64-bit VAST server. See page 14.

Rev. 2.12: (Sept., 2021), software rev. 2.12

	* Added Event Highlights on the timeline on page 96.
	* Redefined Sites into the original substations. See page 195.
	* Added web page link URL favorite icon. See page 66.
	* Added the support for the Video Analysis Alarm (Parking Violation and Restricted Zone detection). See page 98.
	* Added Vehicle detection for smart search II. See page 117.
	* Added encryption for exported videos. See page 96.
	* Added Fisheye dewarp for 3rd-party fisheye cameras through manual calibration. See page 223.
	* Modified Settings > External Devices. See page 202.
	* Added Appendix E for using external Network Audio Devices. See page 235.
	* Added configurable recording path. See page 189.
	* Added Recording Group options and Speed Up (add as offline camera) See page 183.
	* Added Appendix I: Multi-factor Authentication for Access Control. See page 266.

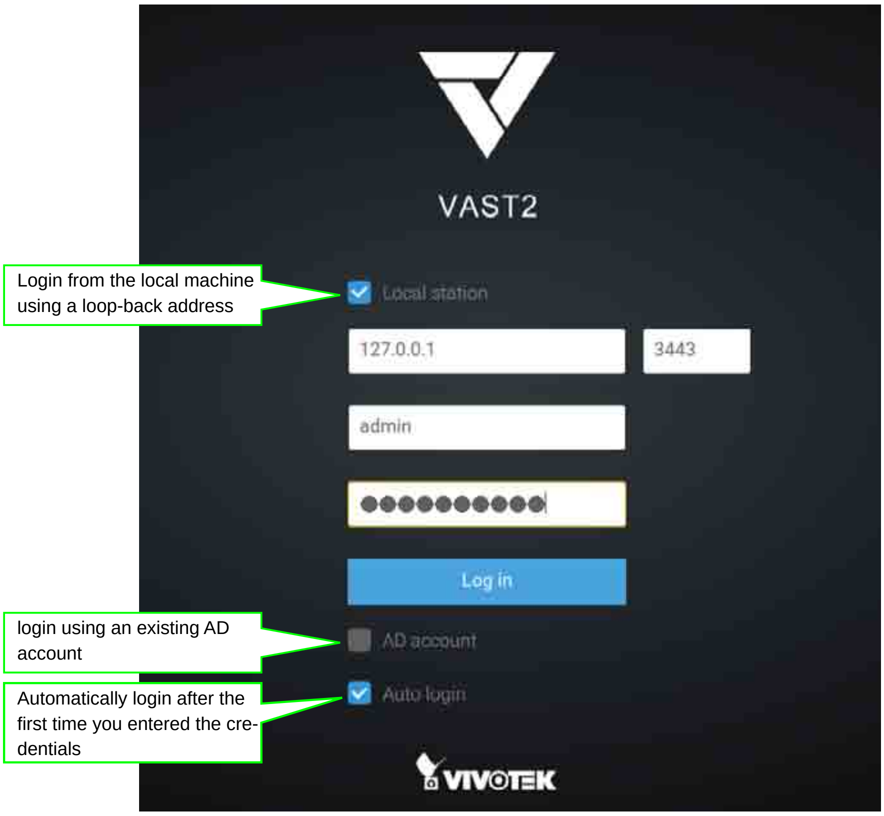
Rev. 2.13: (Feb., 2022), software rev. 2.13

	* Updated new elements on the Dashboard. See page 73.
	* Added Audio device grouping and broadcast schedule. See page 235.
	* Added Virtual trigger. See page 104.
	* Updated Alarm configuration with HTTP request. See page 113.
	* Updated system minimum requirements. See page 49.
	* Updated Charged Features. See page 15.
	* Updated the License activation flow. See page 161.

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 210 for user management and AD count 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.



☑ Local station

127.0.0.1 3443

admin

●●●●●●●●●●

☐ AD account

☑ Auto login

Login from the local machine using a loop-back address

login using an existing AD account

Automatically login after the first time you entered the credentials

Introducing VAST2

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

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

New Features

- Smart Search II Plus: Dynamic Forensic Search
    - Line Crossing: Detection of crossing a user-defined line and direction
    - Loitering: Detection of Loitering in an area for a configurable stay time.
    - Intrusion: Detection of intrusion into a zone or leaving from a zone.
- Smart Tracking: Speed Dome's People Tracking.
- Live Multicast: Reduced network traffic and optimized bandwidth usage.
- CMS Failover: 1+1 redundancy for Central Management server.
- Data Overlay on screen.

Key Features

- License plate recognition solution and data magnet
- Cybersecurity Management Solution
- Smart VCA: AI Powered Video Analytics
- System Overview dashboard
- Multi-sensor display modes
- 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
- 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.

Installation Option - 64-bit VAST2 Server

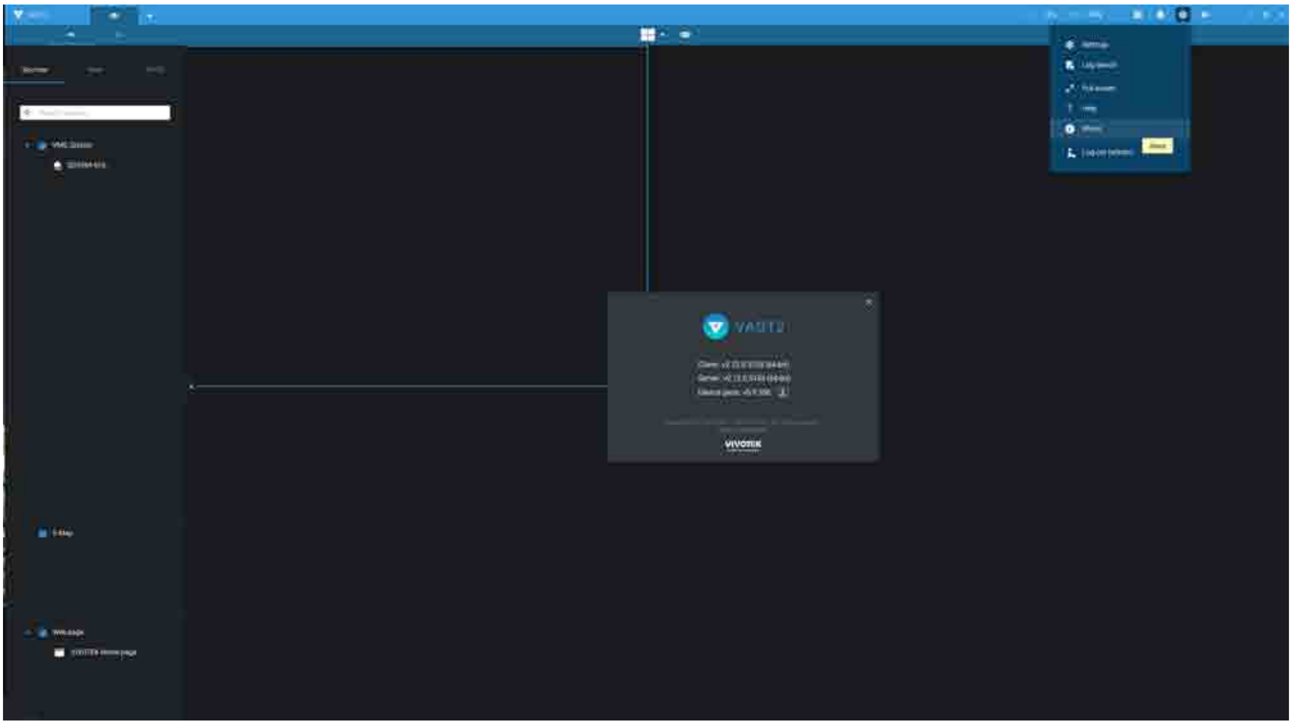
Before revision 2.10, the VAST installation files come as 2 packages:
64-bit option - 1 64-bit VAST2 Client and 1 32-bit VAST2 server.
32-bit option - 1 32-bit VAST2 Client and 1 32-bit VAST2 server.

From revision 2.11, the VAST installation files come as 2 packages:
64-bit option - 1 64-bit VAST2 Client and 1 64-bit VAST2 server.
32-bit option - 1 32-bit VAST2 Client and 1 32-bit VAST2 server.

For users who are using the 32-bit server, you cannot upgrade to 64-bit server unless you uninstall the original 32-bit server. Installing the new 64-bit package does not automatically upgrade the original 32-bit server to 64-bit instance.

You can click Settings > About to find out your current server and client revision.

The 64-bit VAST2 server does not support the installation via a hardware dongle license. Install the 32-bit option if you install a new VAST2 server with hardware dongle license.



Charged Add-on Features

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

Transportation License:

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

POS Implementation:

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

Failover License (substations):

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

Failover License (CMS):

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

Data Magnet License:

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

TCP Message License:

- TCP messages come from external sources (such as access control systems, IoT devices) via the analysis of received TCP messages and used as an alarm triggering source.

Extension License:

- Extension license is used to enable network audio function.

Advanced Feature License:

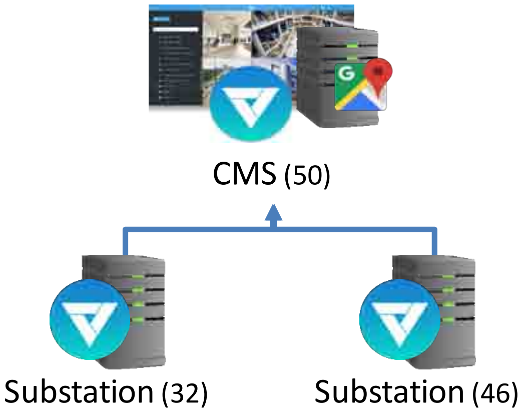
- Advanced License list:
  - Transportation package: Google map / GPS.
  - POS terminal.
  - Failover (Substations)
  - Failover (CMS)
  - TCP message
  - Data Magnet license.
  - Extension

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

Total no. of cameras: 50
Needs 50 packages.

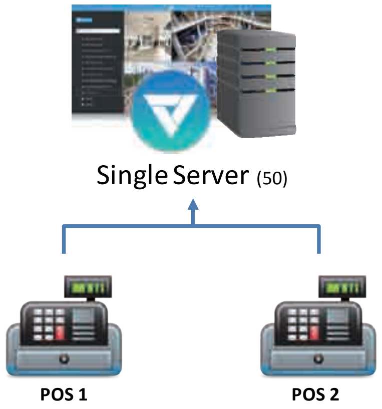
NOTE: camera normal usage licenses are included.



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

NOTE: camera normal usage licenses are included.

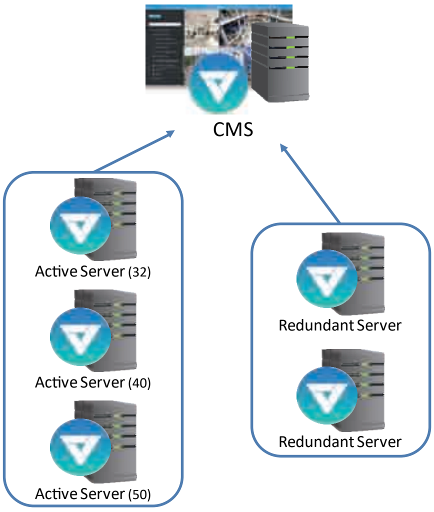
Calculation - POS License



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 (Substations) License

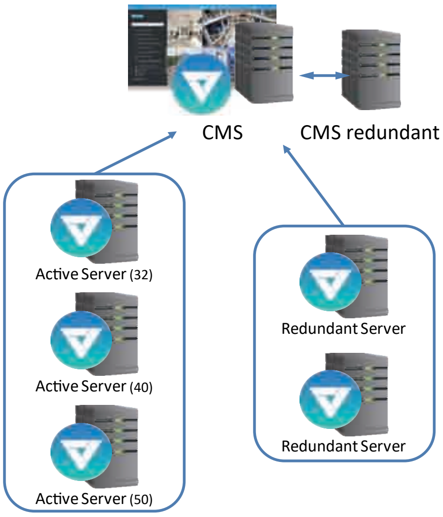


Rule:
No. of channels on the active server hosting the largest no. of cameras x the no. of redundant servers.

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

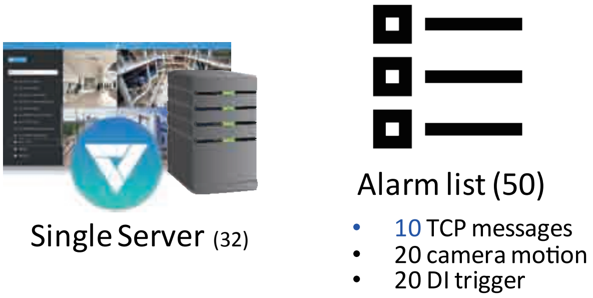
NOTE: 32 camera channels are for free. These licenses do not come with hardware dongle.

Calculation - Failover (CMS) License



Rule:
Adding a CMS redundant server requires a Failover (CMS) license.

Calculation - TCP Message License

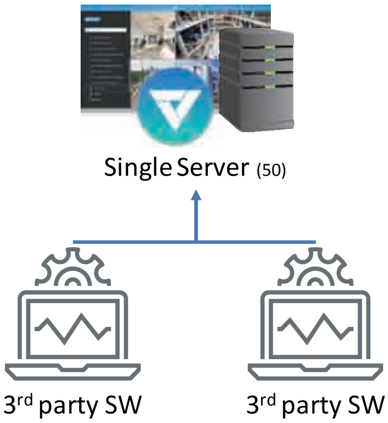


Rule:
The no. of licenses depends on how many alarm rules are using TCP Message as the triggering source.

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

NOTE: 32 camera channels are for free.

Calculation - Data Magnet License

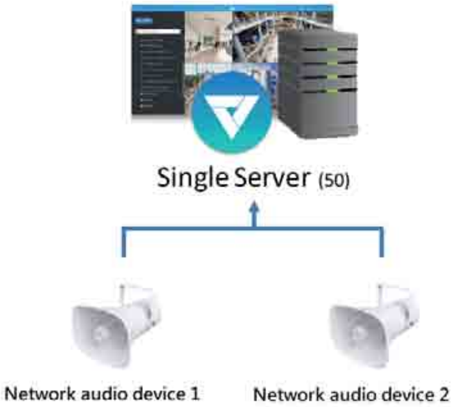


Rule:
The no. of licenses depends on how many Data Magnet sources are implemented.

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

NOTE: 32 camera channels are for free.

Calculation - Extension License (Network Audio Devices)



Rule:
The no. of licenses depends on how many Network Audio devices are implemented.

Total no. of Network Audio Devices: 2
Total no. of cameras: 50
Needs 2 Extension licenses, and 18 normal camera licenses (50 - 32).

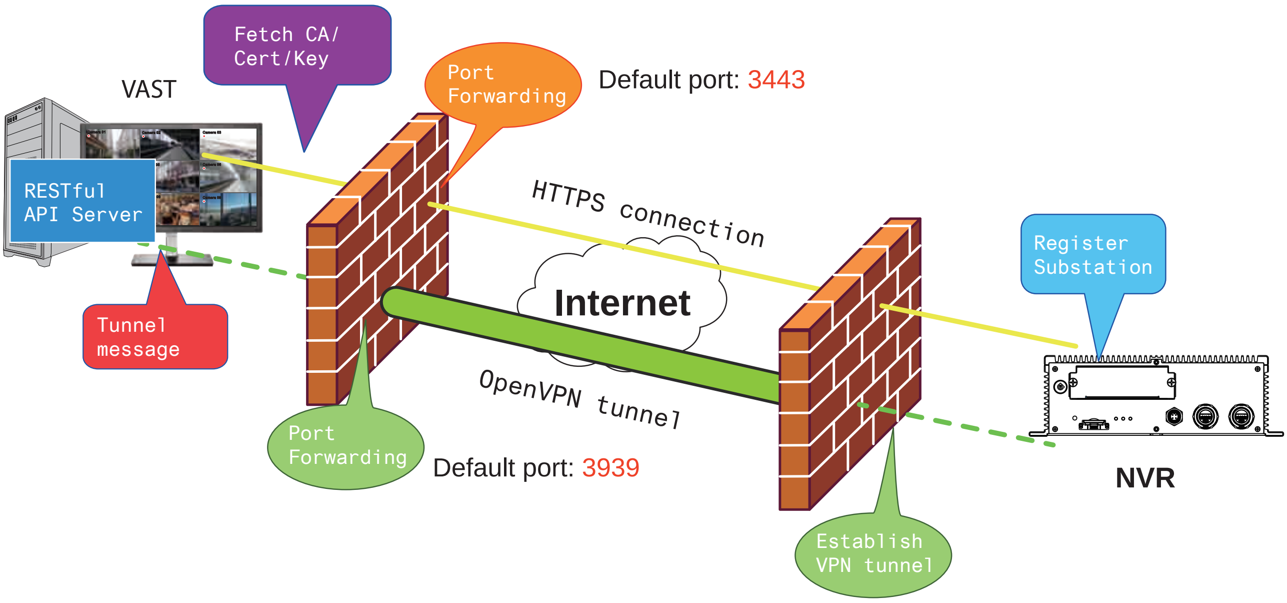
NOTE: 32 camera channels are for free.

Installation Option - OpenVPN

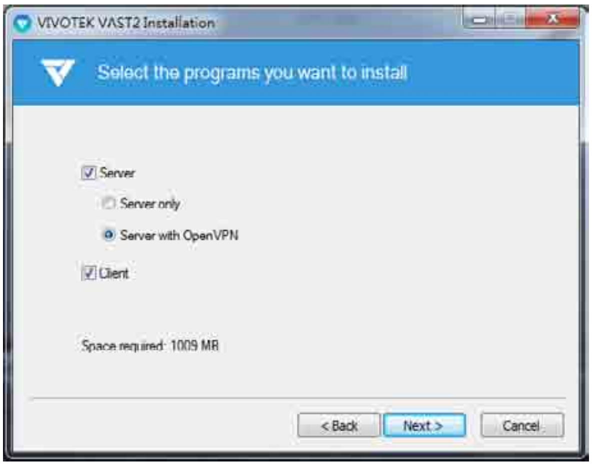
NAT-traversal with OpenVPN

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

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



The sample installation screens are shown below:



VIVOTEK VAST2 Installation
Select the programs you want to install

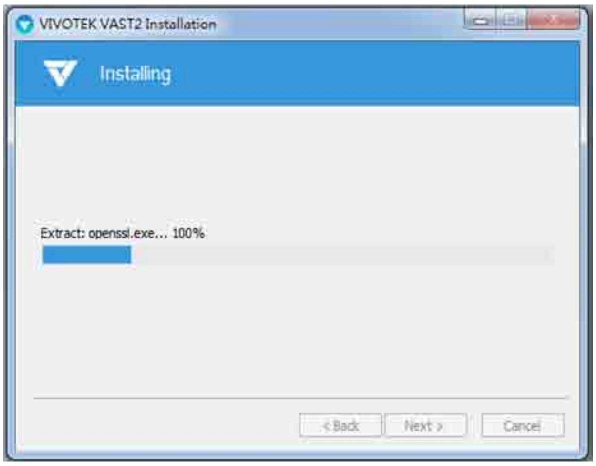
☑ Server

○ Server only

● Server with OpenVPN

☑ Client

Space required: 1009 MB



Extract: openssl.exe... 100%

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

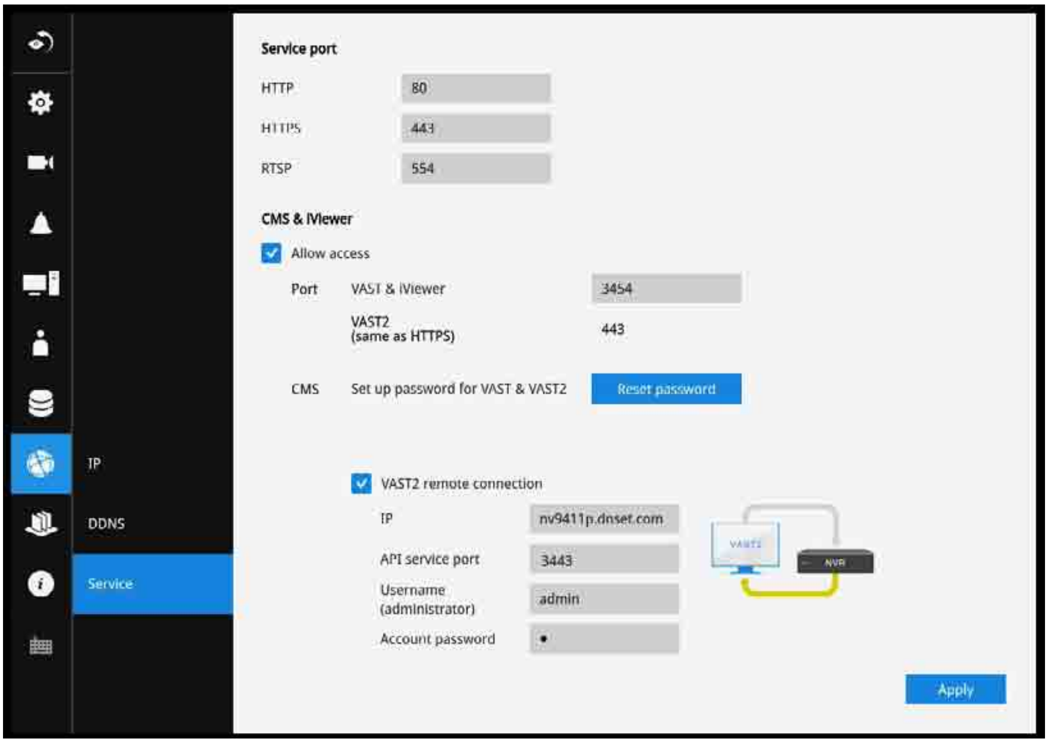
You can edit your VPN IP subnet parameters according to your network configuration. The contents of the editable text file looks like this:

```
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.



Service port

HTTP 80

HTTPS 443

RTSP 554

CMS & iViewer

☑ Allow access

Port VAST & iViewer 3454

VAST2 (same as HTTPS) 443

CMS Set up password for VAST & VAST2 Reset password

☑ VAST2 remote connection

IP nv9411p.dnset.com

API service port 3443

Username (administrator) admin

Account password •

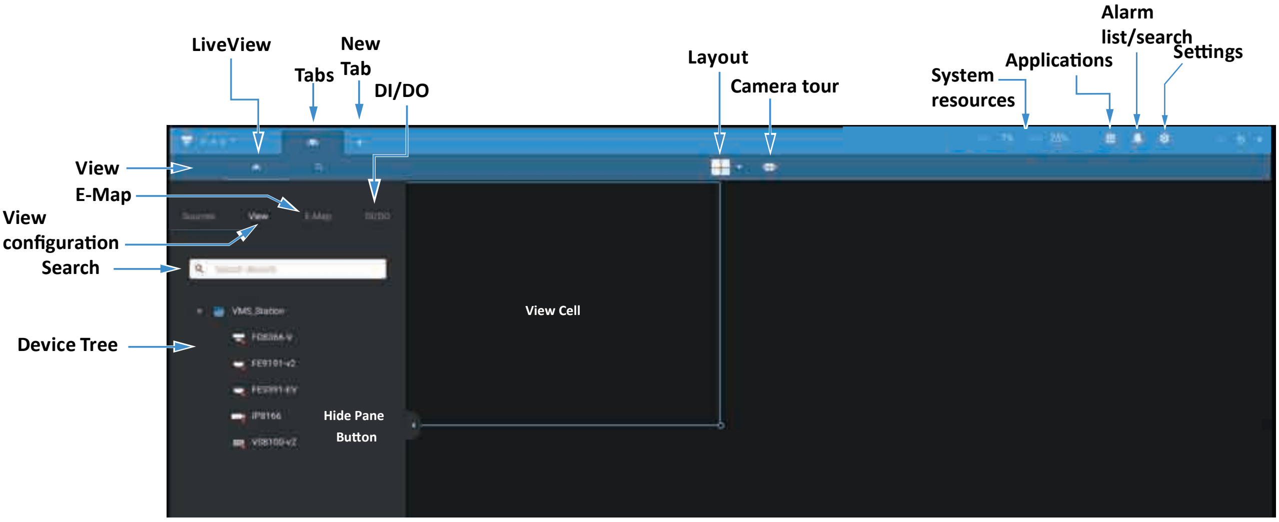
Apply

Chapter 1 Basics:

Control and Elements

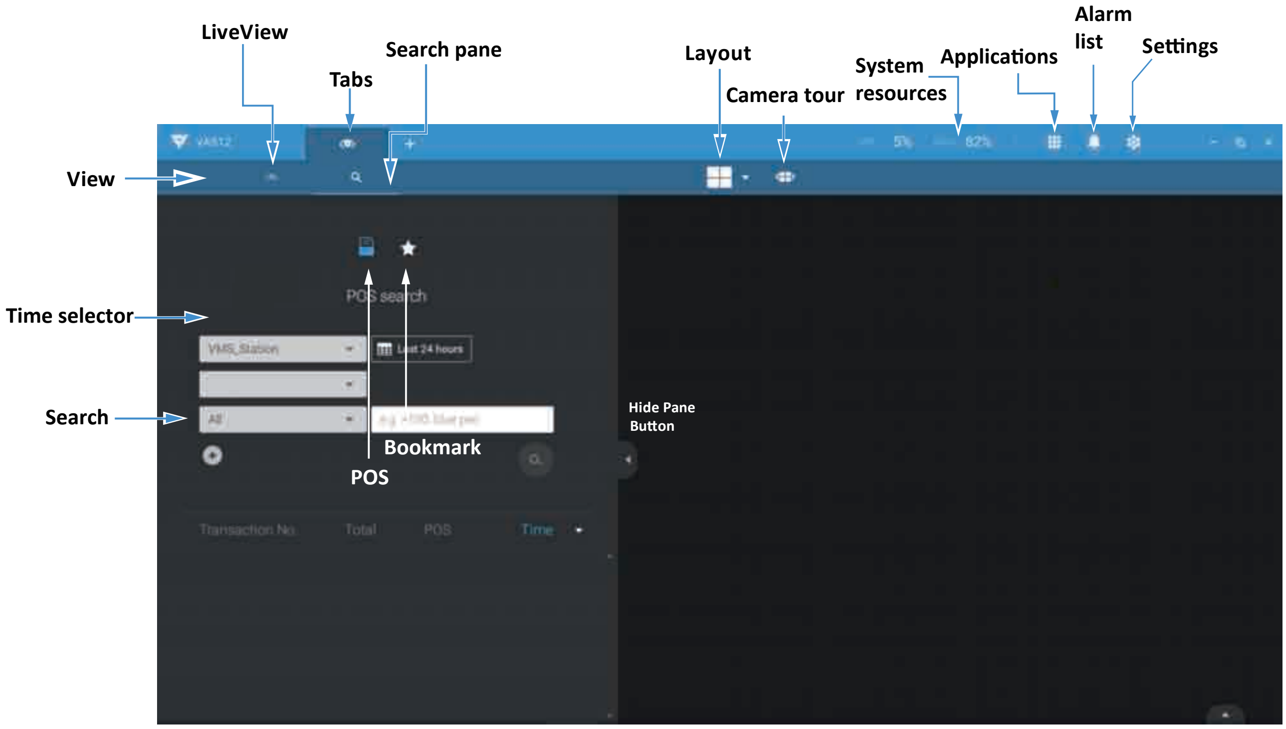
The basic screen elements of VAST live view, playback, and search pane are shown below:

Live view

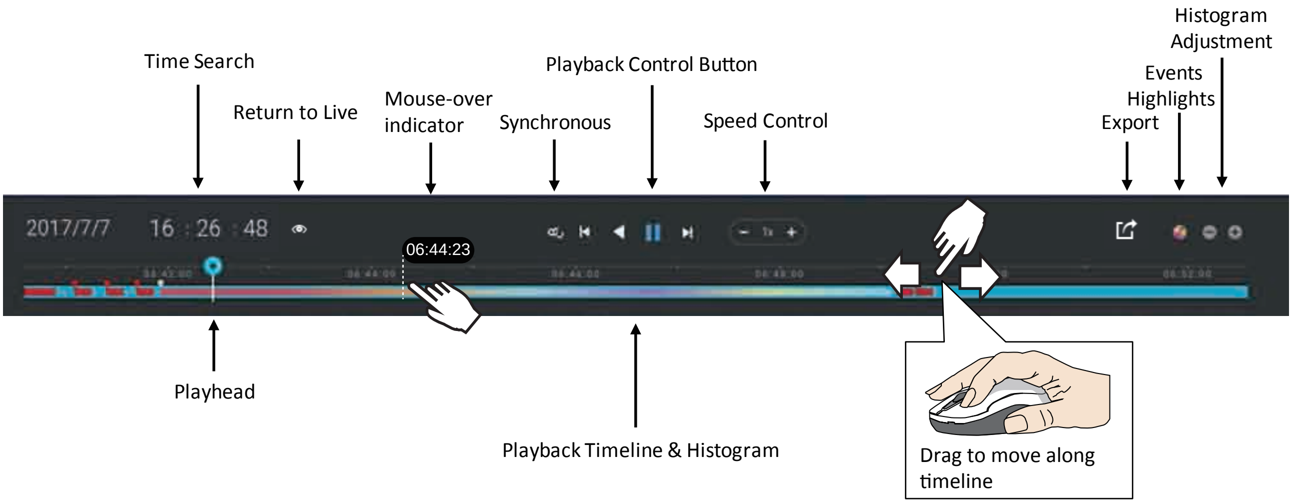


Playback is evoked when a view cell is selected, and you click the Playback button ▶ on the upper right of the view cell.

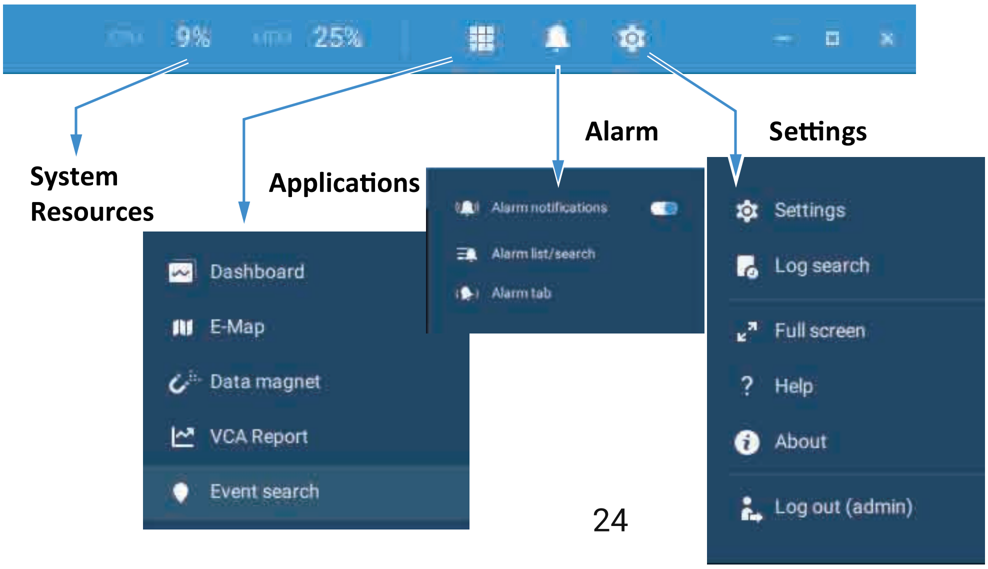
Search Pane



Playback Control

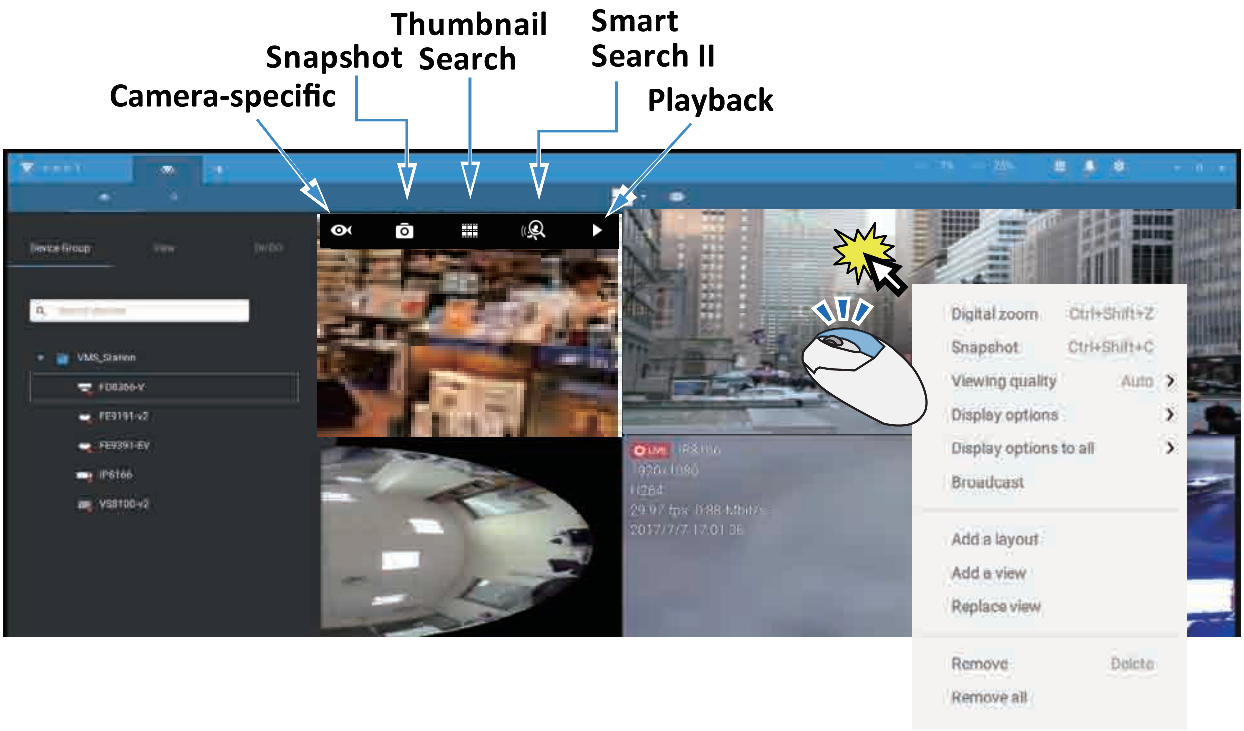


Top Tool Bar



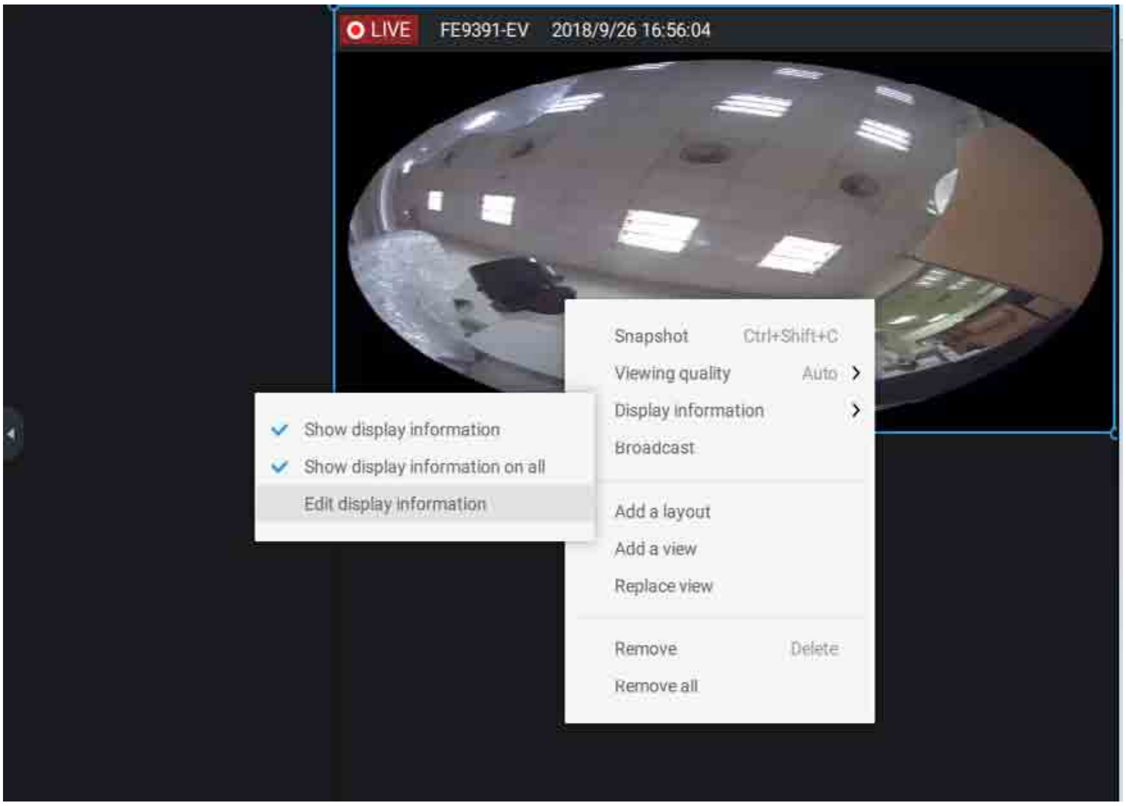
View cell control

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



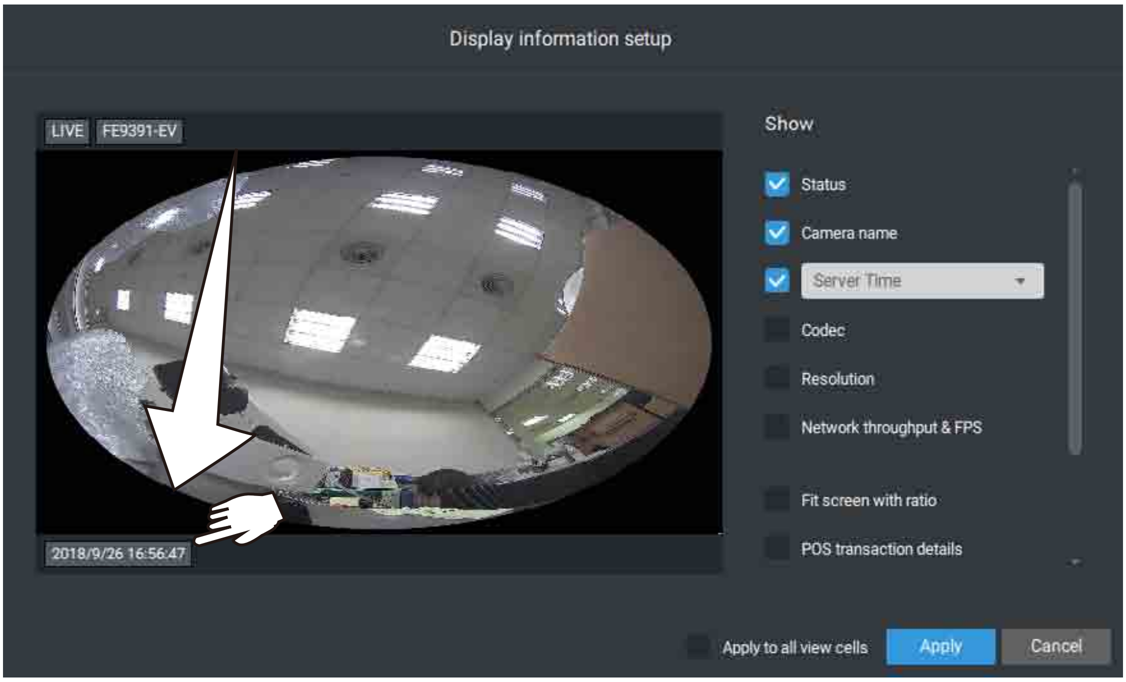
Text overlay

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.

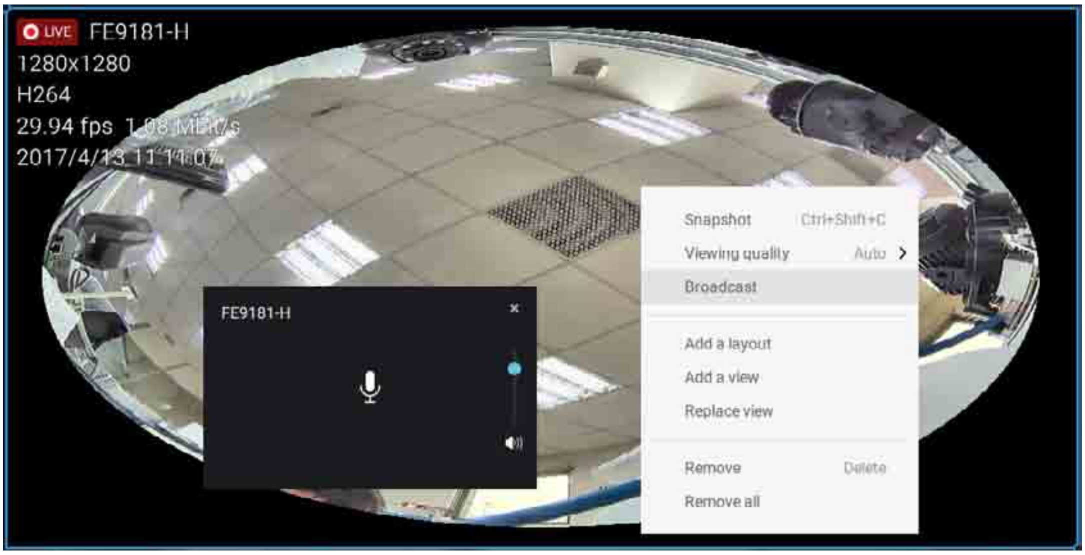
You can apply your current configuration to all view cells by selecting the **Apply to all view cells** checkbox. Note that you can also display the VCA rules and areas on screen.



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.



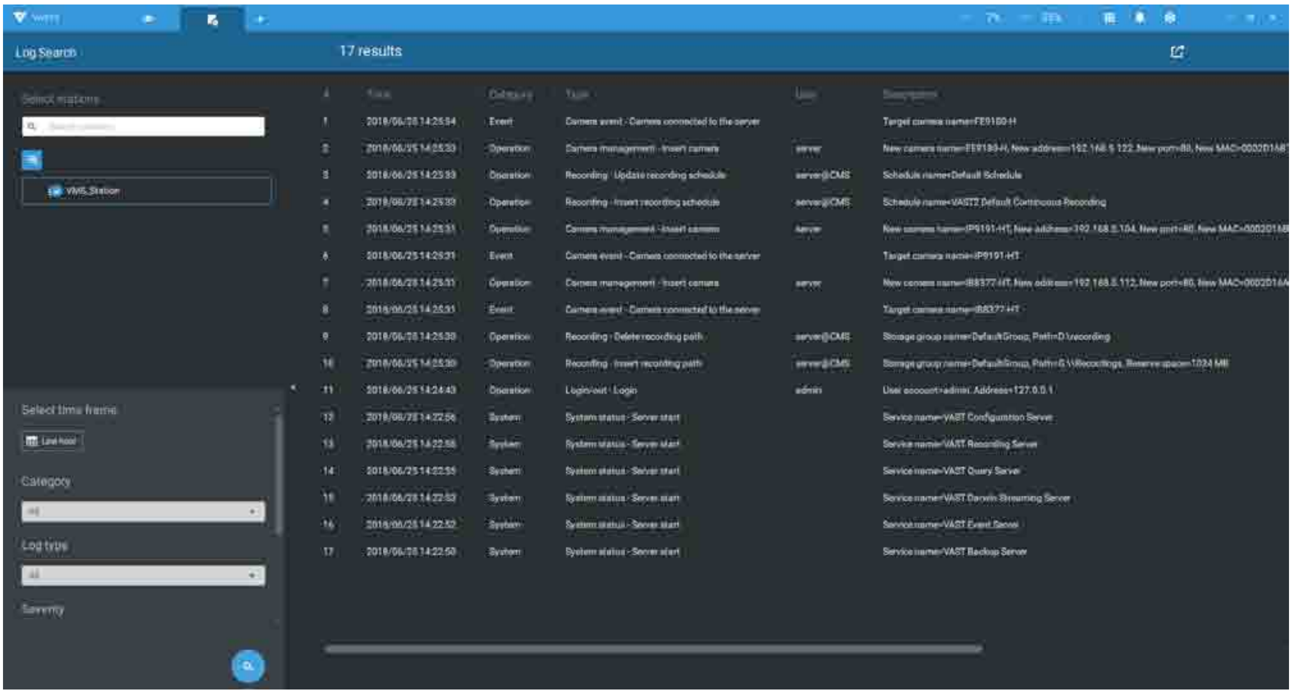
Full Screen

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/station, 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.



17 results

#	Time	Category	Type	User	Description
1	2018/06/25 14:25:34	Event	Camera event - Camera connected to the server		Target camera name=FE9180-H
2	2018/06/25 14:25:33	Operation	Camera management - Insert camera	server	New camera name=FE9180-H, New address=192.168.5.122, New port=80, New MAC=0002D1A8
3	2018/06/25 14:25:33	Operation	Recording - Update recording schedule	server@CMS	Schedule name=Default Schedule
4	2018/06/25 14:25:33	Operation	Recording - Insert recording schedule	server@CMS	Schedule name=VAST2 Default Continuous Recording
5	2018/06/25 14:25:31	Operation	Camera management - Insert camera	server	New camera name=IP9191-HT, New address=192.168.5.104, New port=80, New MAC=0002D1AB
6	2018/06/25 14:25:31	Event	Camera event - Camera connected to the server		Target camera name=IP9191-HT
7	2018/06/25 14:25:31	Operation	Camera management - Insert camera	server	New camera name=IB8377-HT, New address=192.168.5.112, New port=80, New MAC=0002D1A
8	2018/06/25 14:25:31	Event	Camera event - Camera connected to the server		Target camera name=IB8377-HT
9	2018/06/25 14:25:30	Operation	Recording - Delete recording path	server@CMS	Storage group name=DefaultGroup; Path=D:\recording
10	2018/06/25 14:25:30	Operation	Recording - Insert recording path	server@CMS	Storage group name=DefaultGroup, Path=G:\\Recordings, Reserve space=1024 MB
11	2018/06/25 14:24:43	Operation	Login/out - Login	admin	User account=admin, Address=127.0.0.1
12	2018/06/25 14:22:56	System	System status - Server start		Service name=VAST Configuration Server
13	2018/06/25 14:22:55	System	System status - Server start		Service name=VAST Recording Server
14	2018/06/25 14:22:55	System	System status - Server start		Service name=VAST Query Server
15	2018/06/25 14:22:53	System	System status - Server start		Service name=VAST Darwin Streaming Server
16	2018/06/25 14:22:52	System	System status - Server start		Service name=VAST Event Server
17	2018/06/25 14:22:50	System	System status - Server start		Service name=VAST Backup Server

Log Level

Minor：Level 6～8

Normal：Level 3～5

Major：Level 1～2

Operation

VAST2 Type	Log Type	ID	Level	Sample	Extra Parameters											
Login/out	Login	1	3	User Account=admin, Address=127.0.0.1	User account	Address										
	Logout	2	3	User Account=admin, Address=127.0.0.1	User account	Address										
User	Insert user	101	4	New User Name=guest, New Role=PowerUser, New Permission=000F01013F0201070307FFF6F77EFD4E00	New User Name	New Role	New Permission									
	Update user password	104	5	Target User Name=guest	Target User Name											
	Update user privilege	105	5	Target User Name=guest, Target Role=PowerUser, Target Permission=000F01013F0201070307FFF6F77EFD4E00, New User Name=guest, New Role=PowerUser, New Permission=000F01013F0201070307FFF6F77EFD4E00	Target User Name	Target Role	Target Permission	New User Name	New Role	New Permission						
	Delete user	106	3	Target User Name=guest	Target User Name											
	Update user expiration	107	5	Target User Name=guest	Target User Name											
Site	Insert station	201	4	New Station Name=VMS_Station, New Address=172.18.60.31, New Port=3454, New UseSSL=0, New RTSP Port=3454, New Station ID=S_{6312FAC9-FCF4-4573-964D-5F03D083BE54}	New Station Name	New Address	New Port	New UseSSL	New RTSP Port	New Station ID						
	Update station information	202	5	Target Station Name={6312FAC9-FCF4-4573-964D-5F03D083BE54}, Target Address=172.18.60.31, Target Port=3454, Target UseSSL=0, Target RTSP Port=3454, New Station Name={6312FAC9-FCF4-4573-964D-5F03D083BE54}, New Address=172.18.60.31, New Port=3443, New UseSSL=1, New RTSP Port=3443	Target Station Name	Target Address	Target Port	Target UseSSL	Target RTSP Port	New Station Name	New Address	New Port	New UseSSL	New RTSP Port		
	Update station name	203	5	Target Station Name=VMS_Station, New Station Name=CMS	Target Station Name	New Station Name										
	Delete station	204	3	Target Station Name=VMS_Station, Target Station ID=S_{6312FAC9-FCF4-4573-964D-5F03D083BE54}	Target Station Name	Target Station ID										
	Set relay settings	1716	5	Enable=true	Enable											
	Station enable multicast	2416	5	Station name=VMS_Station	Station name											
	Station disable multicast	2417	5	Station name=VMS_Station	Station name											
Camera	Insert camera	205	4	New Camera Name=Door, New Address=172.18.1.129, New Port=80, New MAC=0002D11CC24E, New HTTPS Port=443, New Recording Stream=1	New Camera Name	New Address	New Port	New MAC	New HTTPS Port	New Recording Stream						
	Update camera information	206	5	Target Camera Name=Door, Target Address=172.18.1.129, Target Port=80, Target MAC=0002D11CC24E, Target HTTPS Port=443, Target Recording Stream=1, New Camera Name=IP8362, New Address=172.18.1.129, New Port=80,	Target Camera Name	Target Address	Target Port	Target MAC	Target HTTPS Port	Target Recording Stream	New Camera Name	New Address	New Port	New MAC	New HTTPS Port	New Recording Strea

				New MAC=0002D11CC24E, New HTTPS Port=443, New Recording Stream=1												m
	Delete camera	208	3	Target Camera Name=IP8362	Target Camera Name											
	Set digital output	701	4	Target Camera Name=IP8362	Target Camera Name											
	Set DI/DO name	1715	5	Target Camera Name=IP8362, Target Device=, Reference Name=Alarm	Target Camera Name	Target Device	Reference Name									
	Enable multicast	2414	5	Camera name=SD8362	Camera name											
	Disable multicast	2415	5	Camera name=SD8362	Camera name											
I/O device	Insert External Device	1151	4	Device Name=ADAM-6052, Device Host=172.18.60.70, Device Port=502	Device Name	Device Host	Device Port									
	Remove External Device	1152	3	Device Name=ADAM-6052, Device Host=172.18.60.70, Device Port=502	Device Name	Device Host	Device Port									
	Update External Device	1153	5	Device Name=ADAM-6052, Device Host=172.18.60.70, Device Port=502	Device Name	Device Host	Device Port									
	Set digital output	1154	2	Device Name=ADAM-6052, DO Index=8, Status=Trigger	Device Name	DO Index	Status									
Recording	Manually begin recording	301	2	Target Camera Name=IP8362	Target Camera Name											
	Manually stop recording	302	2	Target Camera Name=IP8362	Target Camera Name											
	Set recording storage	401	4	Storage Group Name=Office	Storage Group Name											
	Insert recording schedule	402	4	Schedule Name=Working Time	Schedule Name											
	Update recording schedule	403	5	Schedule Name=Working Time	Schedule Name											
	Delete recording schedule	404	3	Schedule Name=Working Time	Schedule Name											
	Insert storage group	411	4	Storage Group Name=Office, Cycle=True	Storage Group Name	Cycle										
	Update storage group	412	5	Storage Group Name=Office, Cycle=True	Storage Group Name	Cycle										
	Delete storage group	413	3	Storage Group Name=Office	Storage Group Name											
	Insert recording path	414	4	Storage Group Name=Office, Path=E:\recording, Reserve Space=90112 MB	Storage Group Name	Path	Reserve Space									
	Update recording path	415	5	Storage Group Name=Office, Path=E:\recording, Reserve Space=102400 MB	Storage Group Name	Path	Reserve Space									
	Delete recording	416	3	Storage Group Name=Office, Path=E:\recording	Storage Group Name	Path										

	path															
	Insert camera to the storage group	417	4	Storage Group Name=Office, Camera Name=IP8362	Storage Group Name	Camera Name										
	Delete camera from the storage group	419	3	Storage Group Name=Office, Camera Name=IP8371E	Storage Group Name	Camera Name										
Network	Update server port	1701	5	Server Name=Web, Port=3455	Server Name	Port										
	Set proxy server	1702	5	Enable=True, Address=172.18.60.13, Port=80	Enable	Address	Port									
	Set UPnP	1703	5	UPnP Port Forwarding Enable=False, UPnP Presentation Enable=True	UPnP Port Forwarding Enable	UPnP Presentation Enable										
	Set DDNS server	1704	5	Enable=True, Provider=Dyndns.org(Dynamic)	Enable	Provider										
Alarm	Insert alarm management	408	4	Alarm name=alarm, Trigger list=Motion detection - Motion window 1 of Network Camera, Action list=Set DO status - DO-1 of Network Camera	Alarm name	Trigger list	Action list									
	Update alarm management	409	5	Alarm name=alarm, Trigger list=Motion detection - Motion window 1 of Network Camera, Action list=Set DO status - DO-1 of Network Camera	Alarm name	Trigger list	Action list									
	Delete alarm management	410	3	Alarm name=alarm	Alarm name											
	Stop alarm sound	2408	7	Alarm name=alarm	Alarm name											
	Close alarm notification panel	2409	7	Alarm name=alarm	Alarm name											
	Mute alarm	2411	7	Alarm name=alarm, Duration=10mins,	Alarm name											
PTZ	Camera PTZ, Iris, Focus, Pan, Patrol control	702	7	Target Camera Name=SD9361-EH	Target Camera Name											
	Click on image	703	7	Target Camera Name=SD9361-EH	Target Camera Name											
	Select preset location	704	7	Target Camera Name=SD9361-EH, Preset Name=Door	Target Camera Name	Preset Name										
Backup	Update scheduled backup	1503	5	Enable=true	Enable											
License	Update license information	1717	5	(Empty)												
System	Create directory	1705	4	Target Path=E:\test	Target Path											
	Rename directory	1706	5	Source Path=E:\test, Target Path=E:\recording	Source Path	Target Path										
	Delete directory	1707	3	Target Path=E:\recording	Target Path											
	Update server database path	3401	3	Old path=E:\clientlogs, Target Path=E:\test												
	Insert SMTP	1708	4	Target Address=mail.vivotek.tw, Target Port=25, Target	Target Address	Target Port	Target Order									

	server			Order=0												
	Update SMTP server	1709	5	Target Address=mail.vivotek.tw, Target Port=25, Target Order=0, New Address=mail.vivotek.com, New Port=25, New Order=0	Target Address	Target Port	Target Order	New Address	New Port	New Order						
	Delete SMTP server	1710	3	Target Address=mail.vivotek.tw, Target Port=25, Target Order=0	Target Address	Target Port	Target Order									
	Insert network storage	1711	4	Target Host=rd2fs, Target Domain=vivotek	Target Host	Target Domain										
	Update network storage	1712	5	New Host=rd2fs, New Domain=vivotek, Target Host=rd2fs, Target Domain=vivotek	New Host	New Domain	Target Host	Target Domain								
	Delete network storage	1713	3	Target Host=rd2fs, Target Domain=vivotek	Target Host	Target Domain										
	Watermark settings	2418	5	Status=Disable Status=Enable	Status											
	Import device pack	1721	4	Original version=xxxx, New version=ooo	Original version	New version										
	Import device pack failed	1722	4	Reason=Invalid device pack Reason=Failed to import device pack	Reason											
Live	Add camera	2402	7	New Camera(s) = C1, Total Camera(s) in View= C1,C2	New Camera(s)	Total Camera(s) in View										
	Remove camera	2403	7	Removed Camera(s) = C1, Total Camera(s) in View= C2	Removed Camera(s)	Total Camera(s) in View										
	Replace camera	2404	7	Removed Camera(s) = C1, New Camera(s) = C2,C3 Total Camera(s) in View= C2,C3	Removed Camera(s)	New Camera(s)	Total Camera(s) in View									
View	Add view	2401	5	View Name = View001, Add Camera(s) = C_1	View Name	Add Camera(s)										
	Delete view	2405	5	View Name = View001, Removed Camera(s) = C_1, C_3	View Name	Removed Camera(s)										
	Update view	2406	5	View Name = View001, Removed Camera(s) = C_3, Add Camera(s) = C_1, Total Camera(s) in View= C_1, C_2	View Name	Removed Camera(s)	Add Camera(s)	Total Camera(s) in View								
	Rename view	2407	5	Old View Name = View001, New View Name = View002, Total Camera(s) in View= C1, C_2	Old View Name	New View Name	Total Camera(s) in View									
Data magnet	Add data source	2601	4	Name=Lane, Port=1234, Camera name=FE8173	Name	Port	Camera name									
	Update data source	2602	5	Target name=Lane, Targe port=1234, Target camera name=FE8173, New name=Lane, New port=4321, New camera name=IP8362	Target name	Targer port	Target camera name	New name	New port	New camera name						
	Delete data source	2603	3	Name=Lane	Name											
	Show data	2604	7	Enable=True, Camera name=FE8173	Enable	Camera name										
EMap	Add EMap	3201	7	New EMap(s) = /Dessert, Total EMap(s) in View= /Dessert,/Penguin	New EMap(s)	Total EMap(s) in View										
	Delete EMap	3202	7	Removed EMap(s) = /Dessert, Total EMap(s) in View=	Removed EMap(s)	Total										

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

Event

VAST2 Type	Log Type	ID	Level	Sample	Extra Parameters											
Camera	Camera disconnected from server	1101	2	Target Camera Name=SC8131	Target Camera Name											
	Camera connected to the server	1102	2	Target Camera Name=SC8131	Target Camera Name											
System	Parent station disconnected	1201	2	Target Station Name=VMS_Station	Target Station Name											
	Parent station connected	1202	2	Target Station Name=VMS_Station	Target Station Name											
	Parent station connection lost	1203	2	Target Station Name=VMS_Station	Target Station Name											
	Parent station connection restored	1204	2	Target Station Name=VMS_Station	Target Station Name											
	Substation disconnected	1205	2	Target Station Name=NV9411P	Target Station Name											
	Substation connected	1206	2	Target Station Name=NV9411P	Target Station Name											
	Substation connection lost	1207	2	Target Station Name=NV9411P	Target Station Name											
	Substation connection restore	1208	2	Target Station Name=NV9411P	Target Station Name											
	Start scheduled backup	1501	2	Backup Path=E:\backup, Backup Interval=2018/02/05 00:00:01-2018/02/06 23:58:40	Backup Path	Backup Interval										
	Stop scheduled backup	1502	2	Backup Result Desc=Backup Finish, Backup Interval=2018/02/05 00:00:01-2018/02/06 23:58:40, Backup Latest End Time=2018-02-06 23:58:40.506	Backup Result Desc	Backup Interval	Backup Latest End Time									
	Schedule backup error	1504	2	Media File Source Path=D:\recording\2018-02-04\2-SC8131\1_2018-02-04_000001.3gp, Backup Destination Path=E:\backup, Reason=source is not exist	Media File Source Path	Backup Destination Path	Reason									
Alarm	Alarm trigger	1601	2	Alarm Name=Test, Trigger Type=DO, Action Type=Start to record on	Alarm Name	Trigger Type	Action Type									

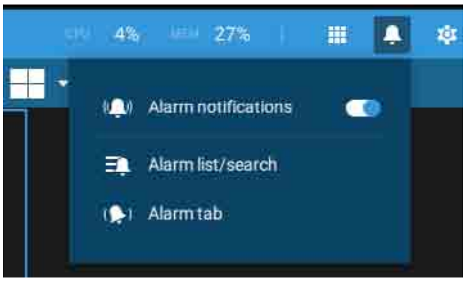
System

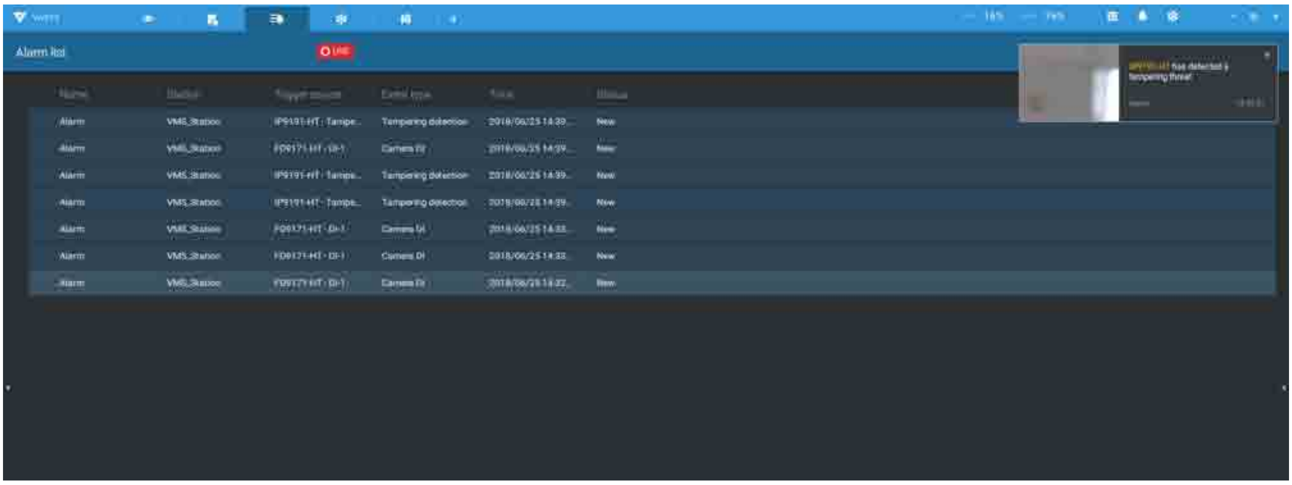
VAST2 Type	Log Type	ID	Level	Sample	Extra Parameters											
System	Server start	1001	1	Service Name=VAST Configuration Server	Service Name											

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

Alarm list

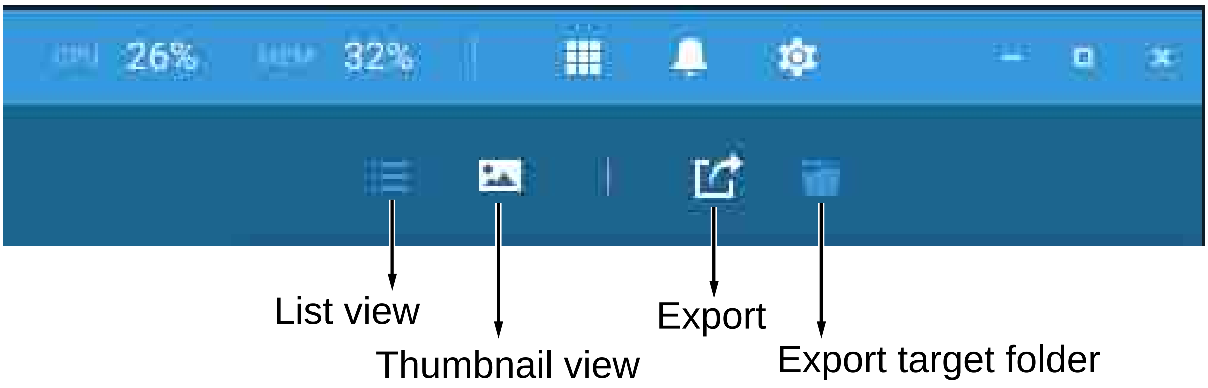
The Alarm list is accessed from the top tool bar. The Alarm list provides easy access to all triggered alarms, such as tampering alarms, alarms reported by VCA analytics, external devices connected via a camera's DI pin, etc.



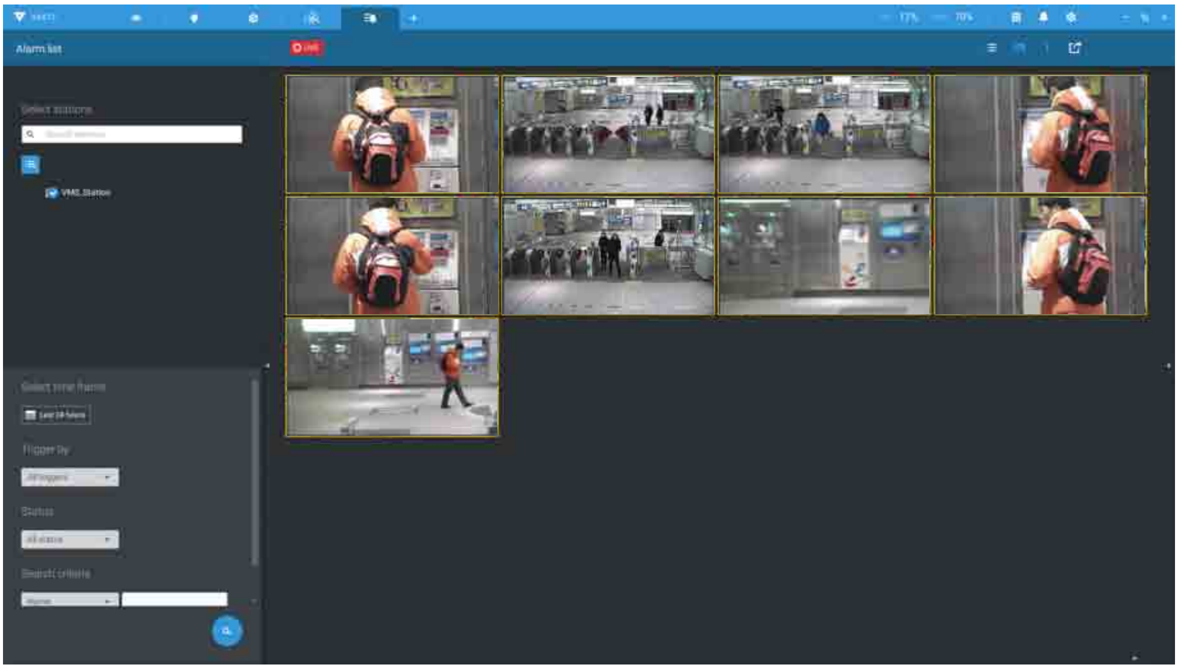


Name	Station	Trigger source	Event type	Time	Status
Alarm	VMS_Station	IP9191-HT : Tampe...	Tampering detection	2018/06/25 14:39...	New
Alarm	VMS_Station	FD9171-HT : DI-1	Camera DI	2018/06/25 14:39...	New
Alarm	VMS_Station	IP9191-HT : Tampe...	Tampering detection	2018/06/25 14:39...	New
Alarm	VMS_Station	IP9191-HT : Tampe...	Tampering detection	2018/06/25 14:39...	New
Alarm	VMS_Station	FD9171-HT : DI-1	Camera DI	2018/06/25 14:33...	New
Alarm	VMS_Station	FD9171-HT : DI-1	Camera DI	2018/06/25 14:33...	New
Alarm	VMS_Station	FD9171-HT : DI-1	Camera DI	2018/06/25 14:32...	New

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



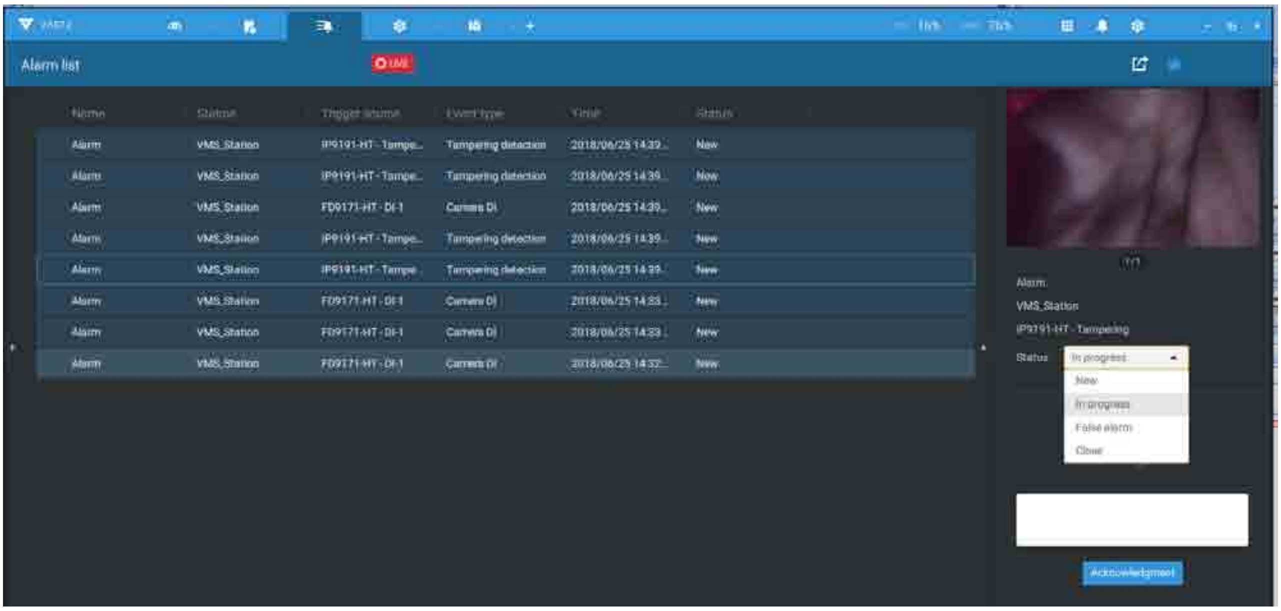
Below is an example of a Thumbnail view.



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 Acknowledegment button.



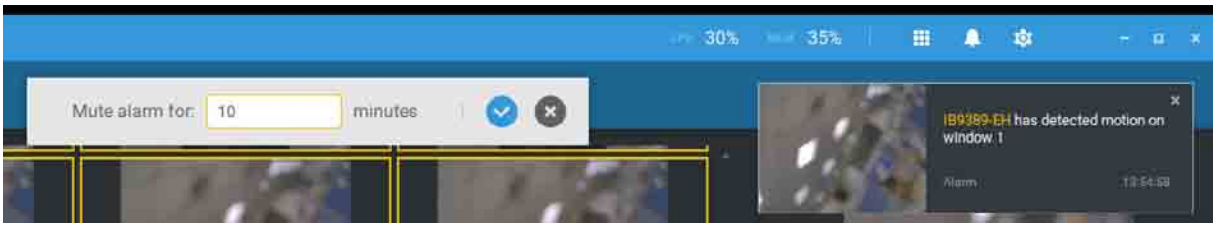
Name	Station	Trigger source	Event type	Time	Status
Alarm	VMS_Station	IP9191-HT - Tampe...	Tampering detection	2018/06/25 14:39...	New
Alarm	VMS_Station	IP9191-HT - Tampe...	Tampering detection	2018/06/25 14:39...	New
Alarm	VMS_Station	FD9171-HT - DI-1	Camera DI	2018/06/25 14:39...	New
Alarm	VMS_Station	IP9191-HT - Tampe...	Tampering detection	2018/06/25 14:39...	New
Alarm	VMS_Station	IP9191-HT - Tampe	Tampering detection	2018/06/25 14:39...	New
Alarm	VMS_Station	FD9171-HT - DI-1	Camera DI	2018/06/25 14:33...	New
Alarm	VMS_Station	FD9171-HT - DI-1	Camera DI	2018/06/25 14:33...	New
Alarm	VMS_Station	FD9171-HT - DI-1	Camera DI	2018/06/25 14:32...	New

Alarm
VMS_Station
IP9191-HT - Tampering
Status: In progress

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.



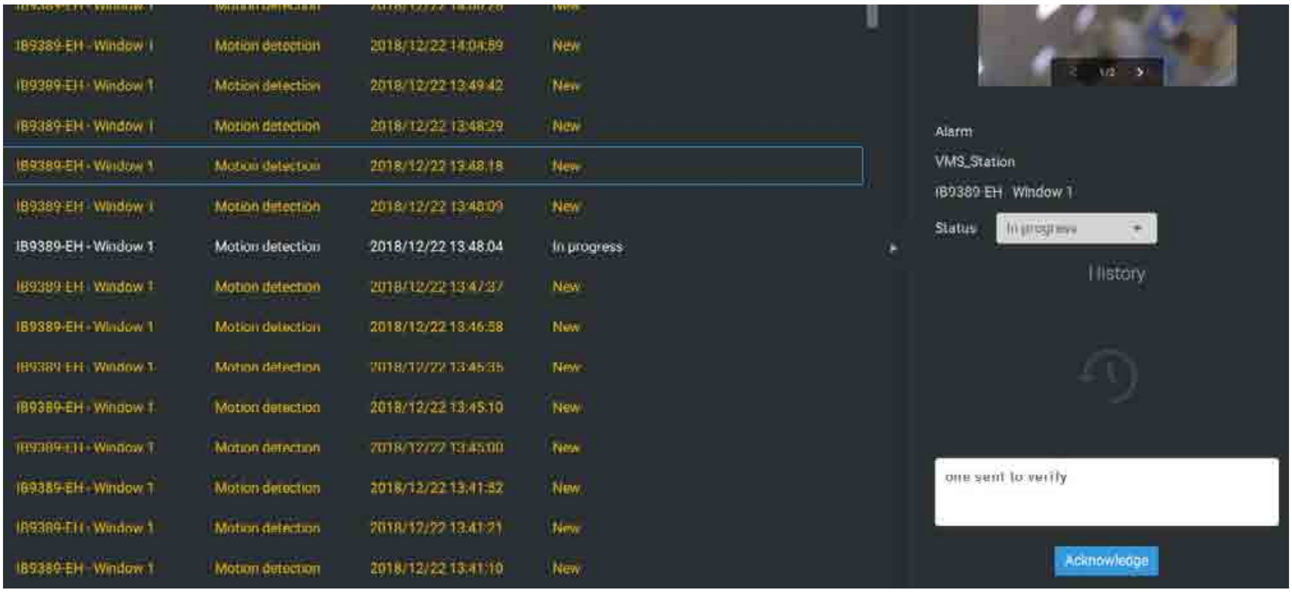
Mute alarm for: 10 minutes

IB9389-EH has detected motion on window 1

Alarm 13:54:58

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.



IB9389-EH - Window 1	Motion detection	2018/12/22 14:04:59	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:49:42	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:48:29	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:48:18	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:48:09	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:48:04	In progress
IB9389-EH - Window 1	Motion detection	2018/12/22 13:47:37	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:46:58	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:46:35	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:45:10	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:45:00	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:41:52	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:41:21	New
IB9389-EH - Window 1	Motion detection	2018/12/22 13:41:10	New

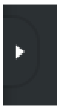
Alarm

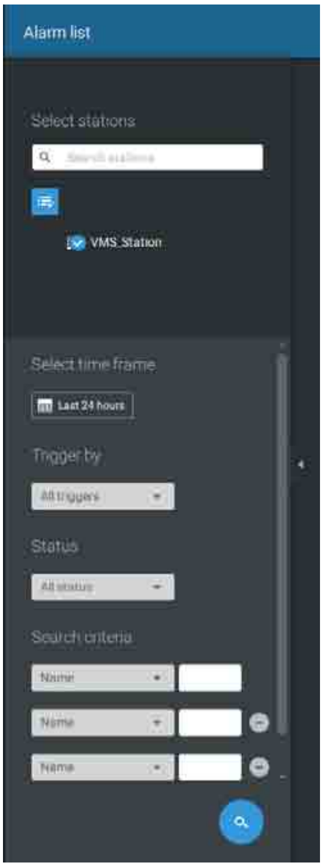
VMS_Station

IB9389-EH Window 1

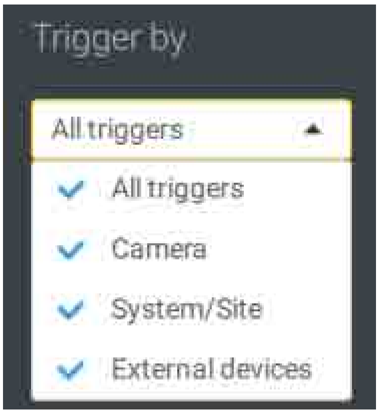
Status: In progress

one sent to verify

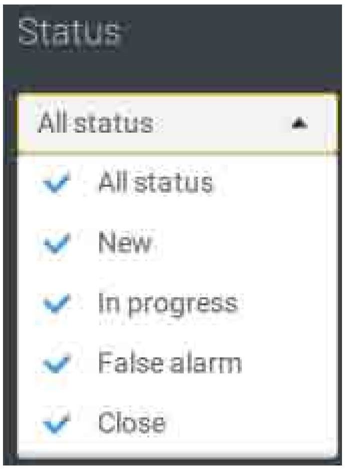




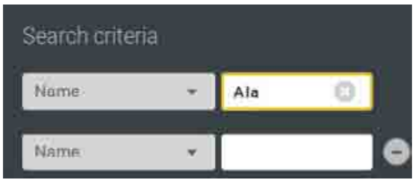
To find alarms of specific types, time of occurrences, and alarm status, click the side tab to reveal the search panel.



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



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


Search criteria

Name: Ala

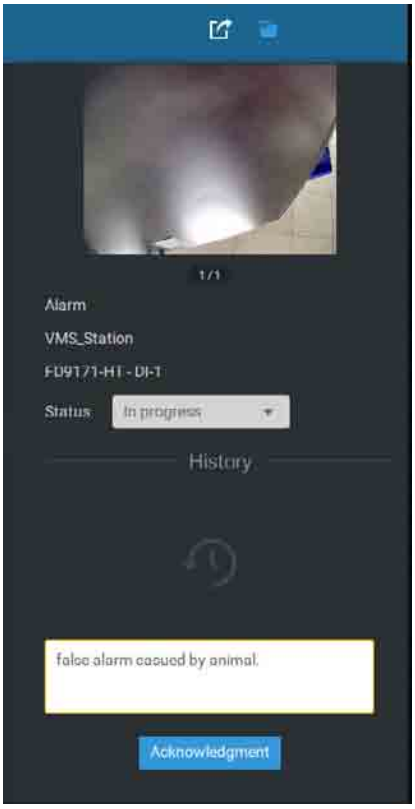
Name:

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

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

You can use the Export button 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.


1/1

Alarm

VMS_Station

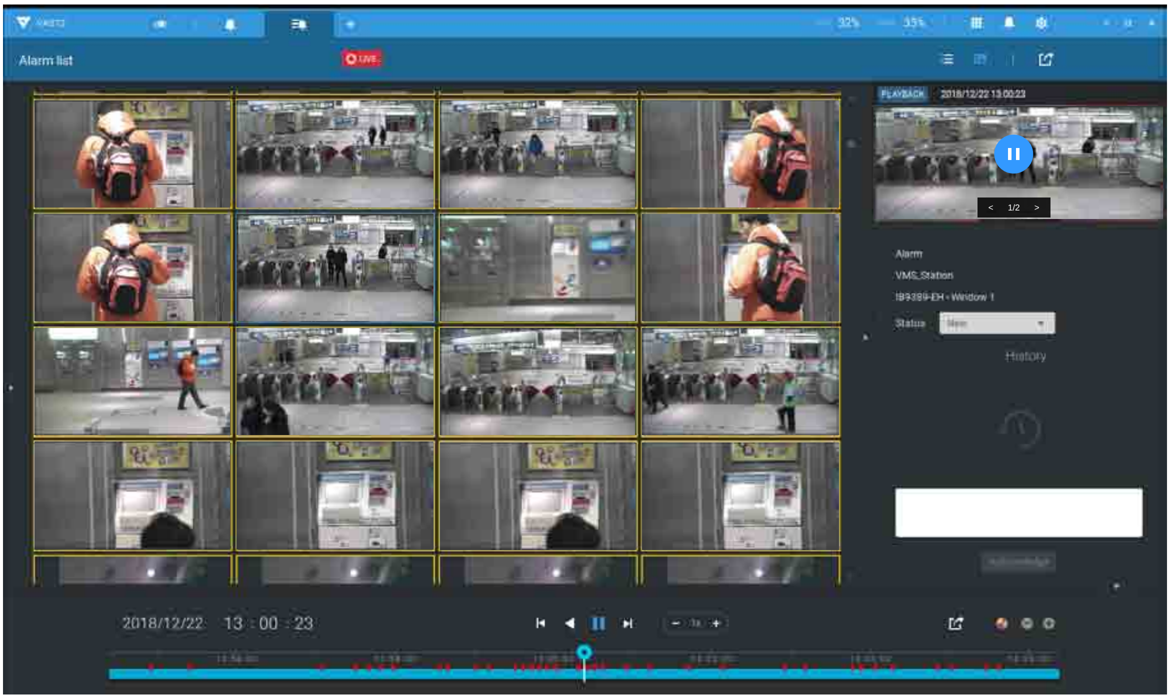
FD9171-HT - DI-1

Status: In progress

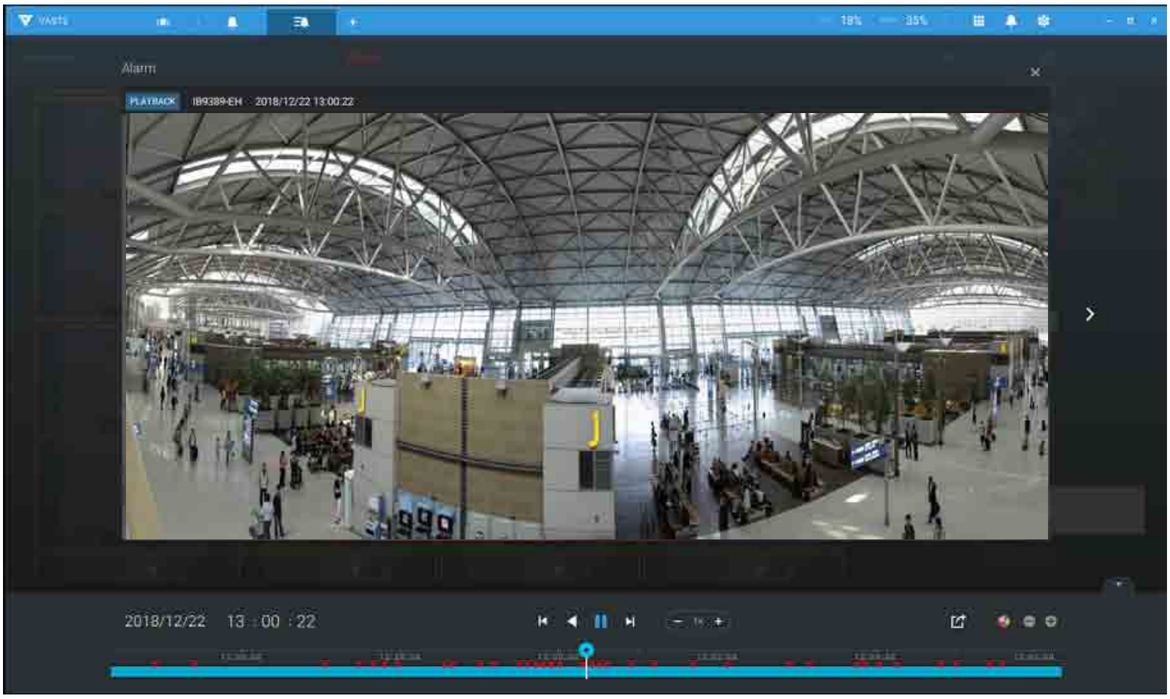
History

false alarm caused by animal.

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.

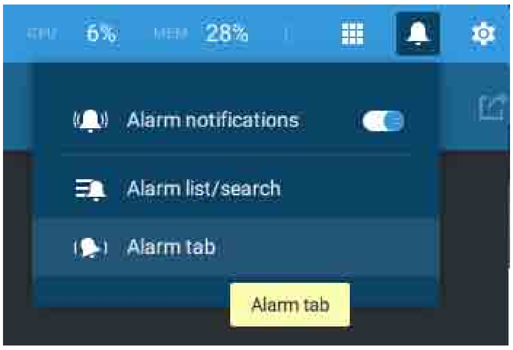


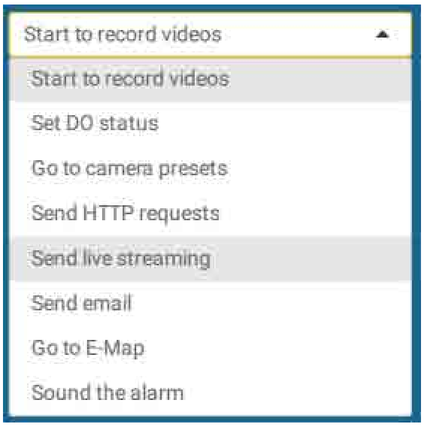
Double-click on the small playback screen again to bring it to the full view. The playback control, time line, export, and alarm tags will be available on screen.



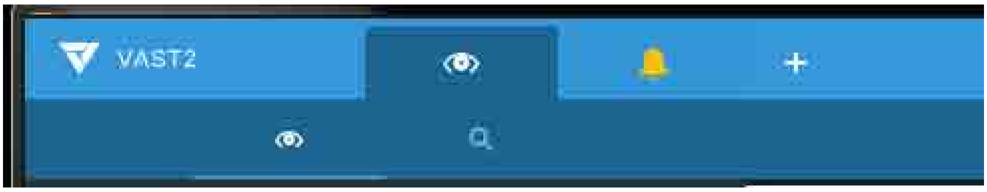
Alarm tab

The Alarm tab is an automated streaming window displaying live videos brought 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 types of alarms.

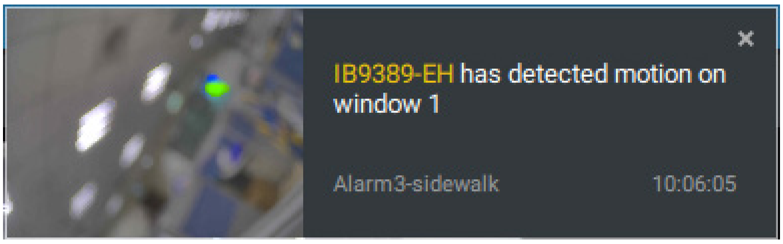




When a live streaming is sent by an alarm, an orange ringing bell icon will display.



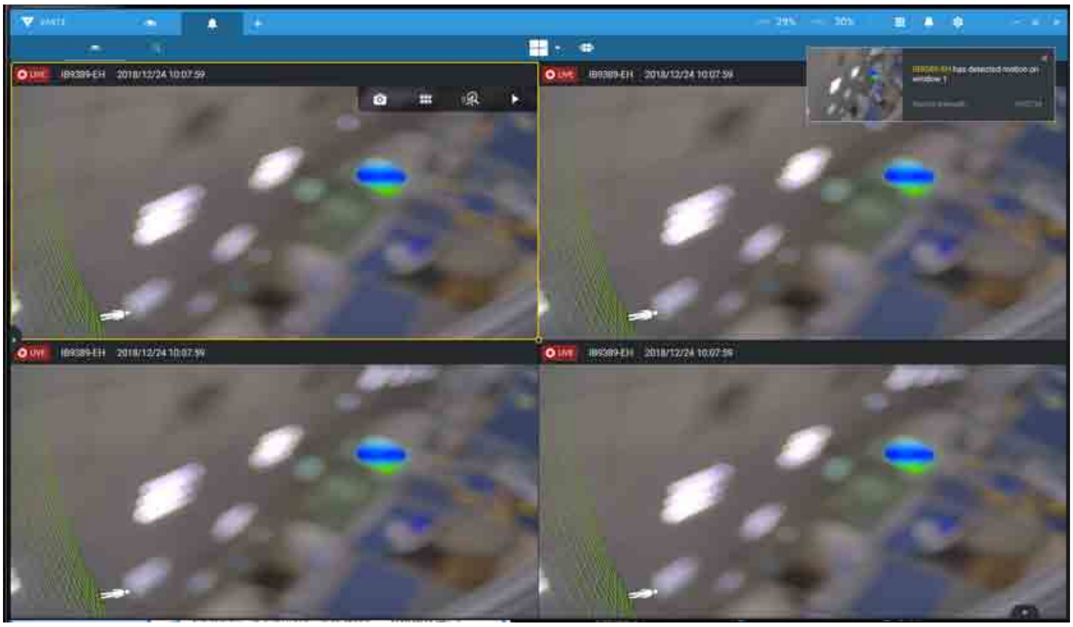
An alarm prompt will also display on the screen.



IB9389-EH has detected motion on window 1

Alarm3-sidewalk 10:06:05

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

Smart search II			
- Configuration page			
Delete detection range			Esc

Bookmark search			
Select more bookmarks	Ctrl (Win) / Command (MacOS)		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
Stations Management			
Rename selected station			F2
Remove selected station 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 (Win) / Command (MacOS)		m
Designate the selected alarms as false alarms	Ctrl (Win) / Command (MacOS)		f
Select all alarms	Ctrl (Win) / Command (MacOS)		a
Select one or multiple alarms	Ctrl (Win) / Command (MacOS)		left mouse button
Select multiple alarms		Shift	left mouse button
Select different alarms			Up/Down/Left/Right

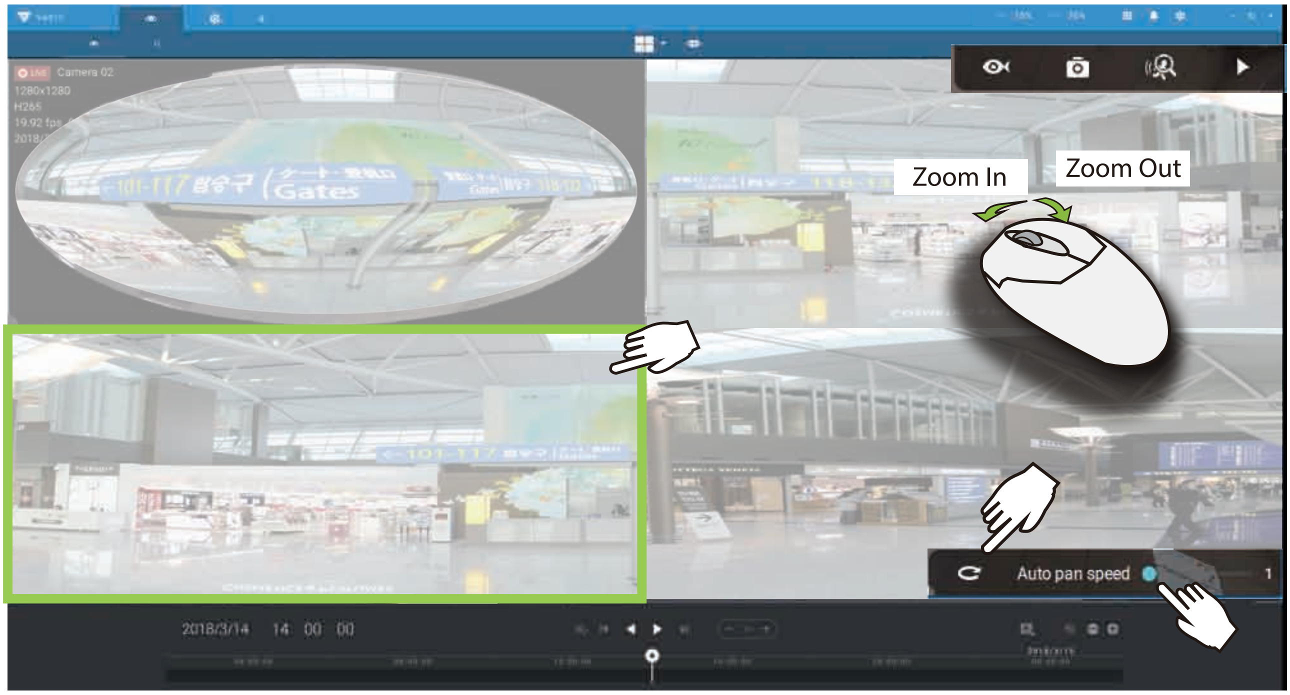
View Cell Elements

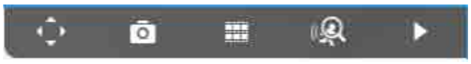
On a view cell, the control elements are different with different types of network cameras. 3 major types are listed below with applicable screen elements:

1. **Fixed** cameras: Snapshot - Thumbnail search - Smart search - Replay.

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

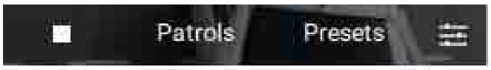
   The Auto pan function applies only to the Regional views. Select a regional view, and click the Auto pan button. The Regional view will pan from side to side to cover more viewable regions. If a fisheye is mounted on wall, a regional view with auto pan can cover a panoramic view region.



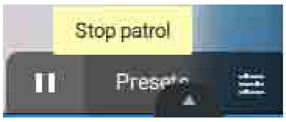
3. **PTZ** cameras:  PTZ - Snapshot - Thumbnail search - Smart search - Replay. For information about PTZ control, refer to the discussion on PTZ on page 88.

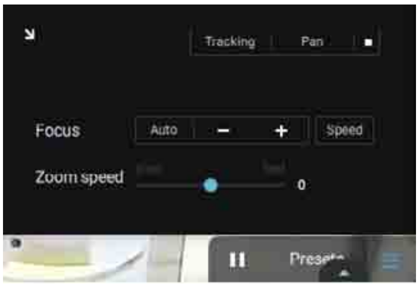
To exert PTZ control, first click on this button to enable PTZ control.

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

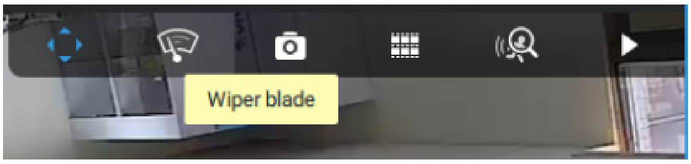


Click Patrols or Presets if these have been configured on the PTZ camera. You will need to open a web console to the camera to configure preset positions.



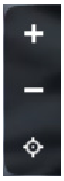


The PTZ settings tab allows you to enable PTZ Tracking and the Pan functions. You can also adjust the Zoom and Focus speed, or manually adjust the focus. Please refer to the camera User Manual for more information about these functions.



For speed dome cameras that come with a 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.

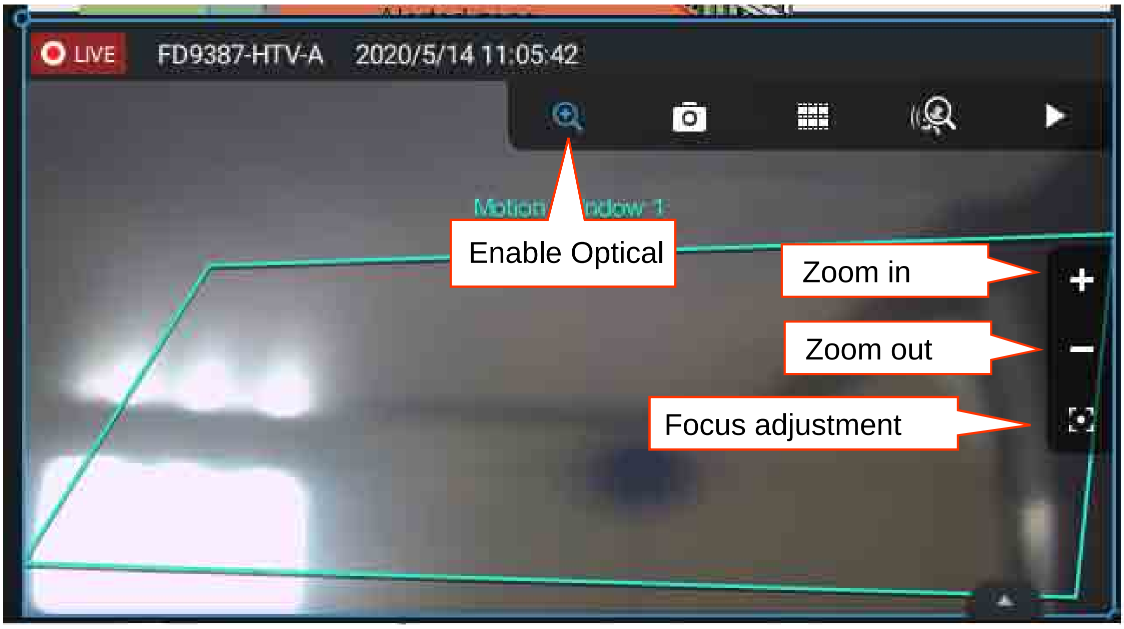


When PTZ is enabled, the zoom buttons and a home button are displayed on the right hand side of the view cell.

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

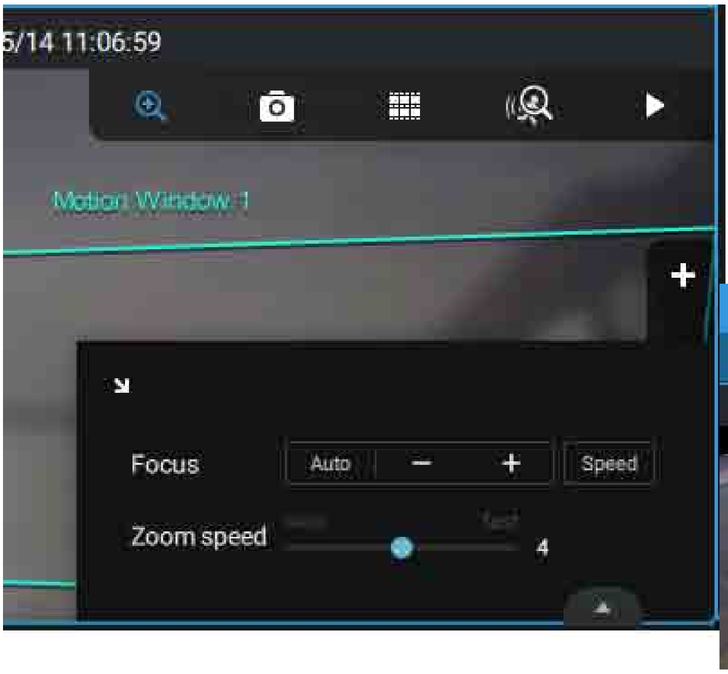
3. **Motorized lens** cameras: Enable Optical - Snapshot - Thumbnail search - Smart search - Replay.

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



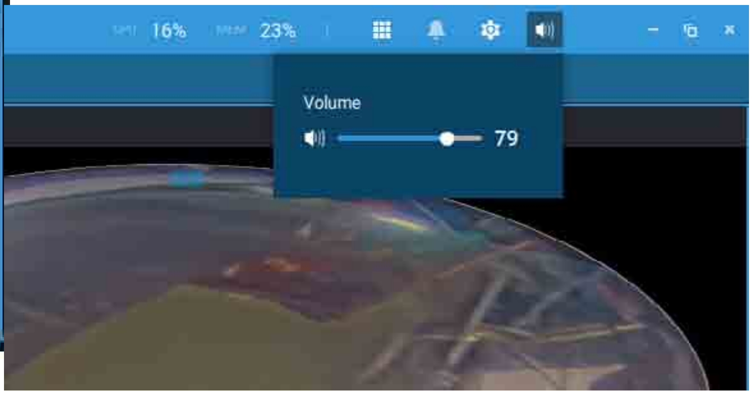
Click on the Focus adjustment button to bring out the focus panel. If you find the image is out of focus, you can use the +, -, or Auto buttons to regain the best image focus.

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



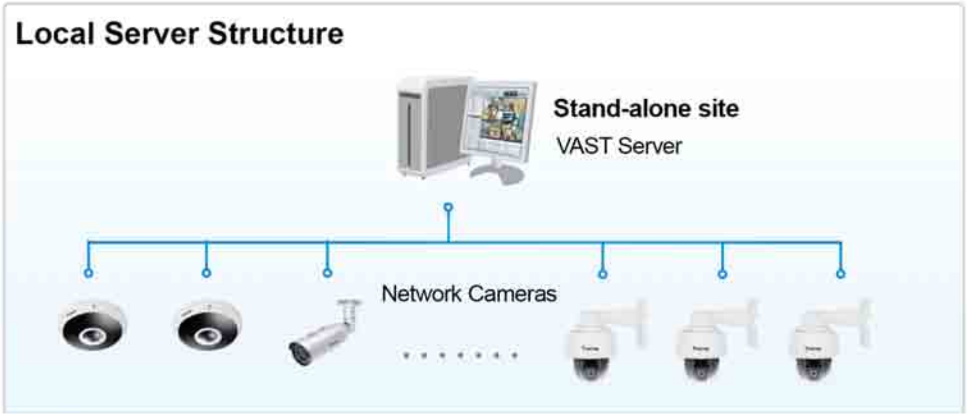
Audio

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



VAST Server and Client Components

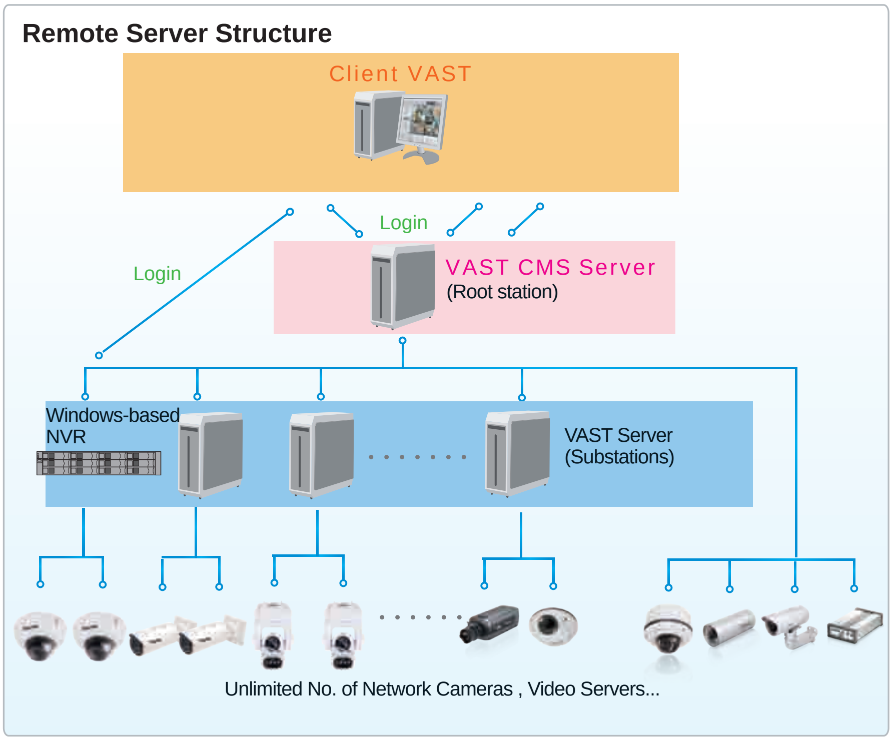
VAST2 Server provides a centralized management site for video recording. Users can login and modify the server's configuration, edit the server's recording storage, configure schedules and many other functions. You can browse the recorded video database and video clips related to specific events on the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



For users who manage large-scale surveillance deployments, please plan the hierarchical structure first. Then you can start to add cameras to each station and connect these 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 station. All the functions can be simultaneously performed on one single station.



Please refer to the Stations 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 core installation type is not supported.)		
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*
Network Interface Card	Ethernet, 1Gbit recommended***		

* The size of volume group depends on the total recording server throughput. Throughput of each volume group must exceed the total bit rate of cameras recorded in that specific volume group.

** 256 CH without Smart VCA, 128 CH with Smart VCA.

*** 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.

***** If cameras are all running VCA, the max. number of recording channels will be 128.

VAST 2 Liveview & Playback				
Operating System		Windows Server 2012, 2016 / Windows 10, 7 / MacOS 10.15 Catalina (Server core installation type is not supported.)		
Clients (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		

* Independent graphics card is necessary when using Windows Server OS.

* Display requirements of the 3MP fisheye camera is equal to a 720P camera.

** Display requirements of the 5MP fisheye camera is equal to a 1080P camera.

*** Please use a dual-channel memory configuration.

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

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

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

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

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

32-CH, VGA, about 1 week recording: 750 GB

64-CH, VGA, about 1 week recording: 1TB x 2

32-CH, 2-megapixel, about 1 week recording: 2TB x 2

64-CH, 2-megapixel, about 1 week recording: 2TB x 4

Chapter 2 Starting Up

Double-click the VAST2 icon VAST2 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).

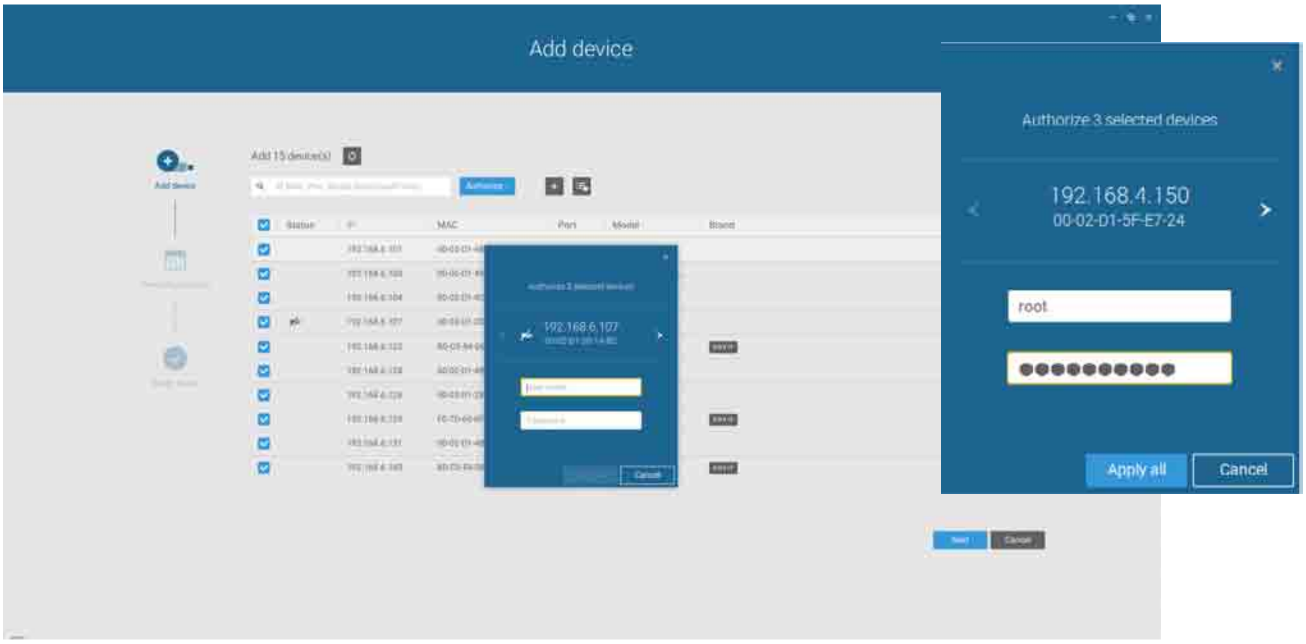
Use the + Add device button to manually add a camera with its known IP or domain name.

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.



Authorize 3 selected devices

192.168.4.150
00-02-D1-5F-E7-24

root

●●●●●●●●●●

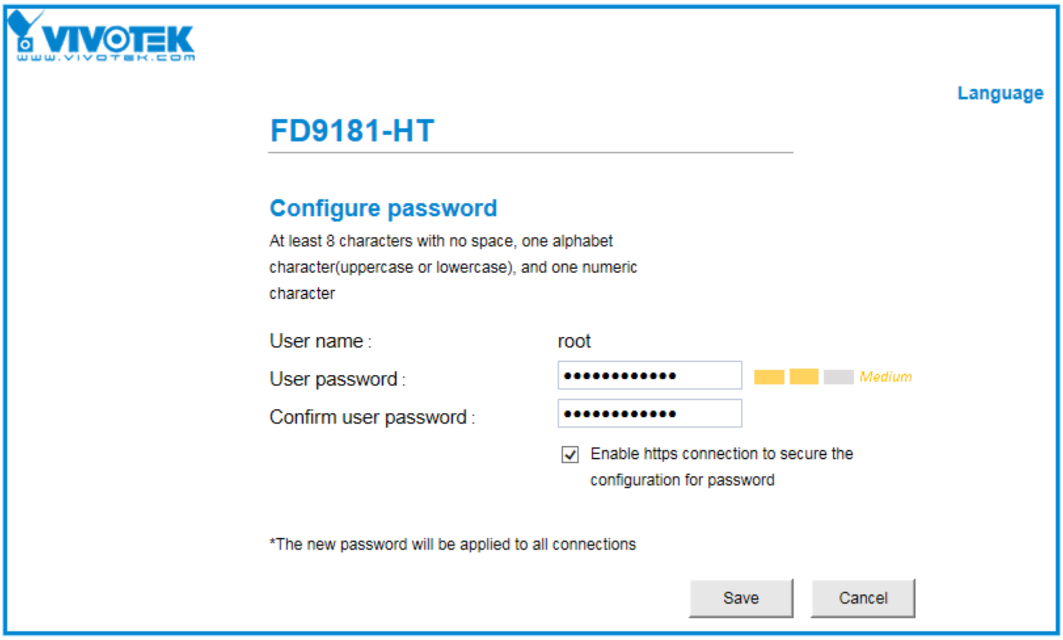
2-1. Selecting Devices

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.



FD9181-HT

Configure password

At least 8 characters with no space, one alphabet character(uppercase or lowercase), and one numeric character

User name : root

User password : ••••••••••••• Medium

Confirm user password : •••••••••••••

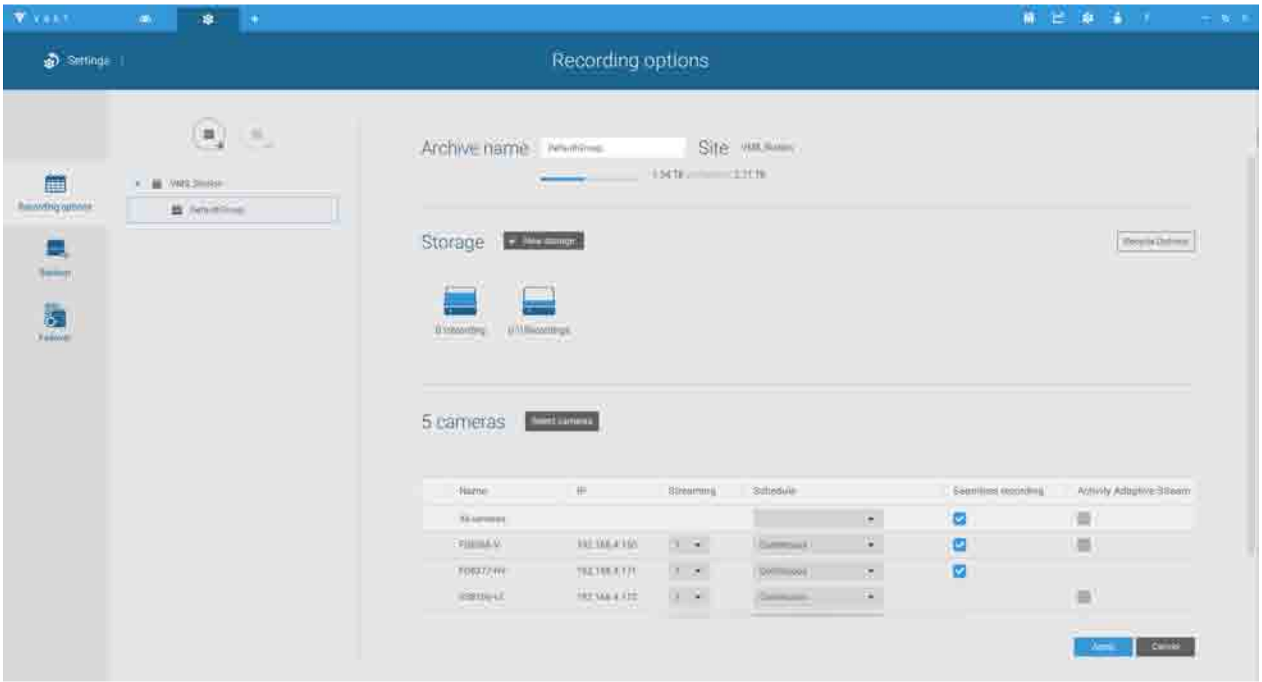
☑ Enable https connection to secure the configuration for password

*The new password will be applied to all connections

2-2. Recording Options

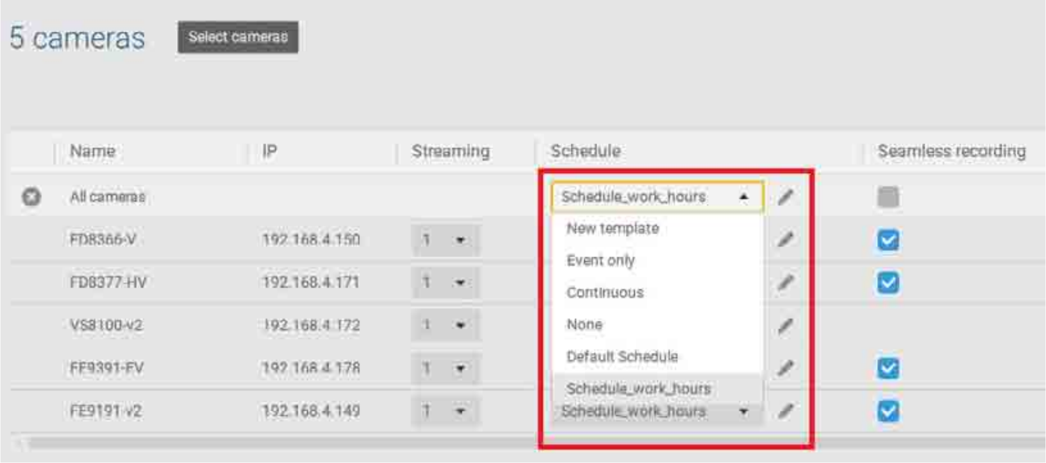
Click **Settings** > **Recording** > **Recording options**. The Recording options window will prompt.

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



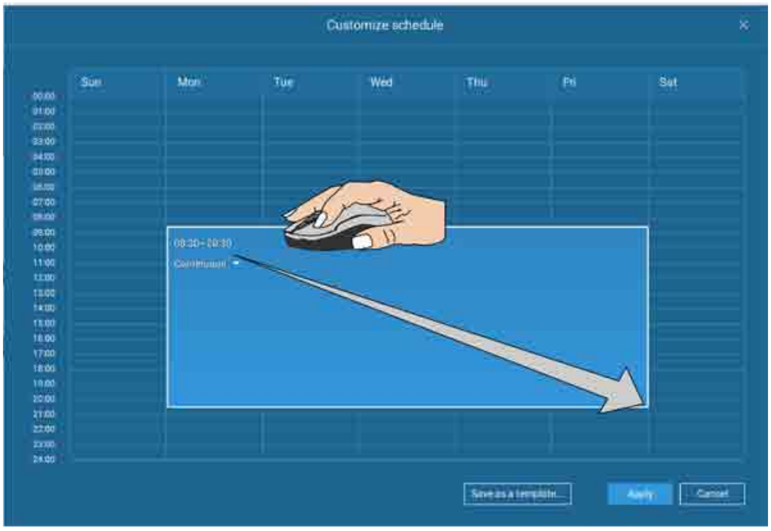
Click on the Schedule column on the Camera list for a recording option: **Continuous recordings**, **Events only**, **None**, or **Default Schedule**, or **New template**. You can apply a schedule template for all cameras or configure individual schedules for different cameras. When using the Event-triggered 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.



5 cameras Select cameras

Name	IP	Streaming	Schedule	Seamless recording
All cameras			Schedule_work_hours ▴	☐
FD8366-V	192.168.4.150	1 ▾		☑
FD8377-HV	192.168.4.171	1 ▾		☑
VS8100-v2	192.168.4.172	1 ▾		
FE9391-EV	192.168.4.178	1 ▾		☑
FE9191-v2	192.168.4.149	1 ▾	Schedule_work_hours ▾	☑



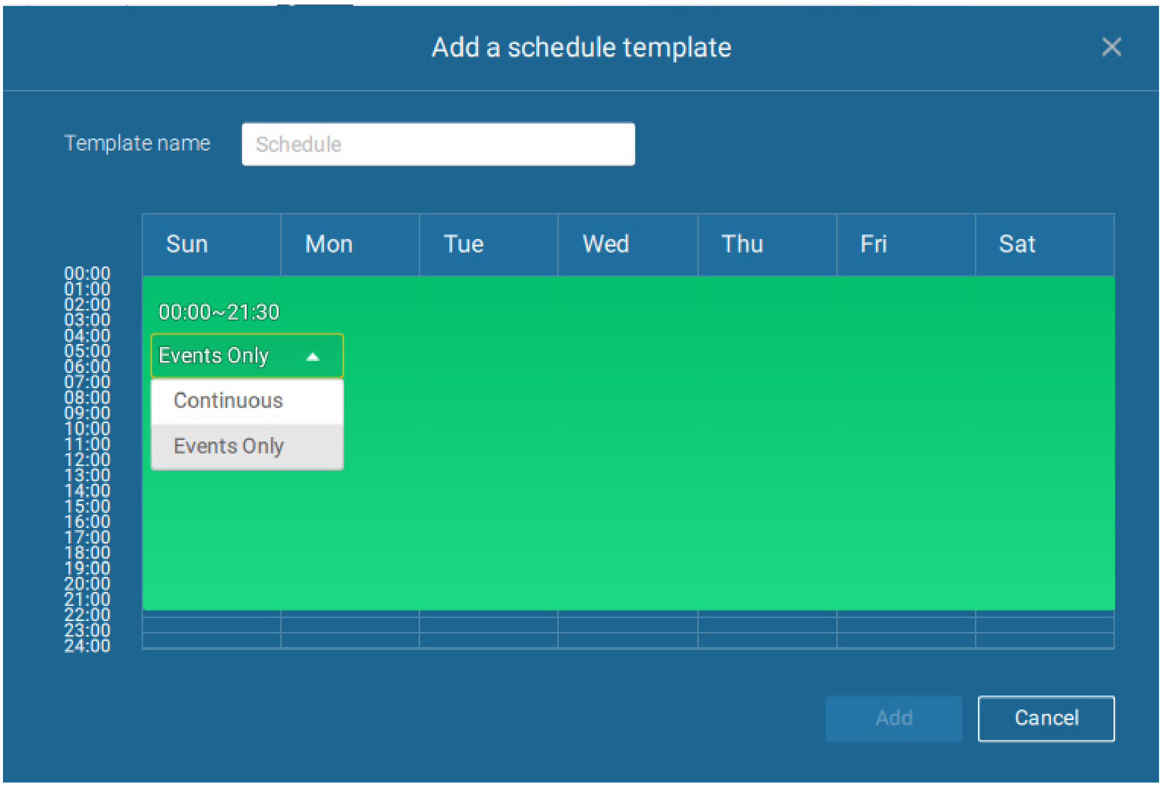
08:30~20:30
Continuous

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

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

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

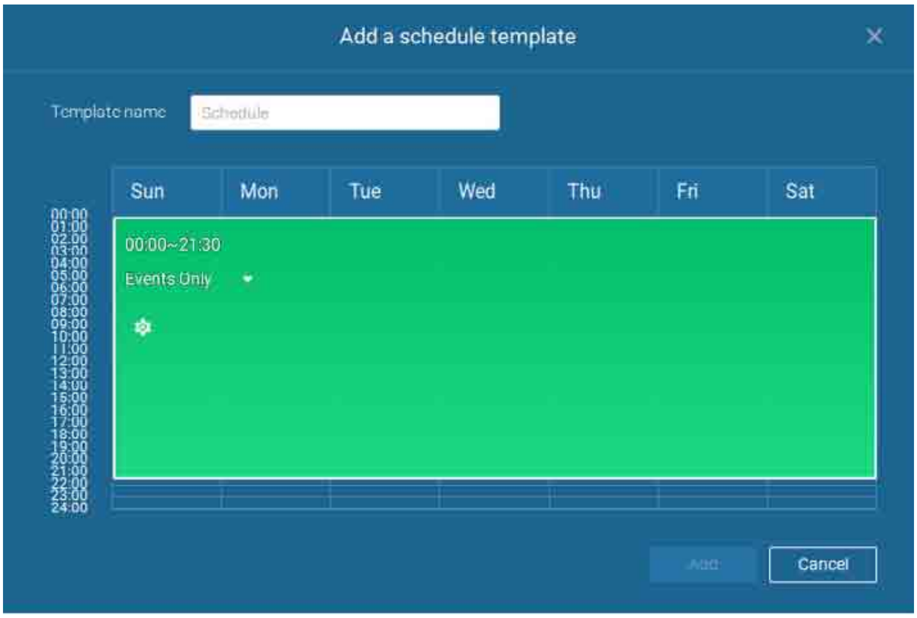
If the **Events only** option is selected for the new template, you can determine what kinds of events will trigger the recording. Use the pull-down menu to select Events only.



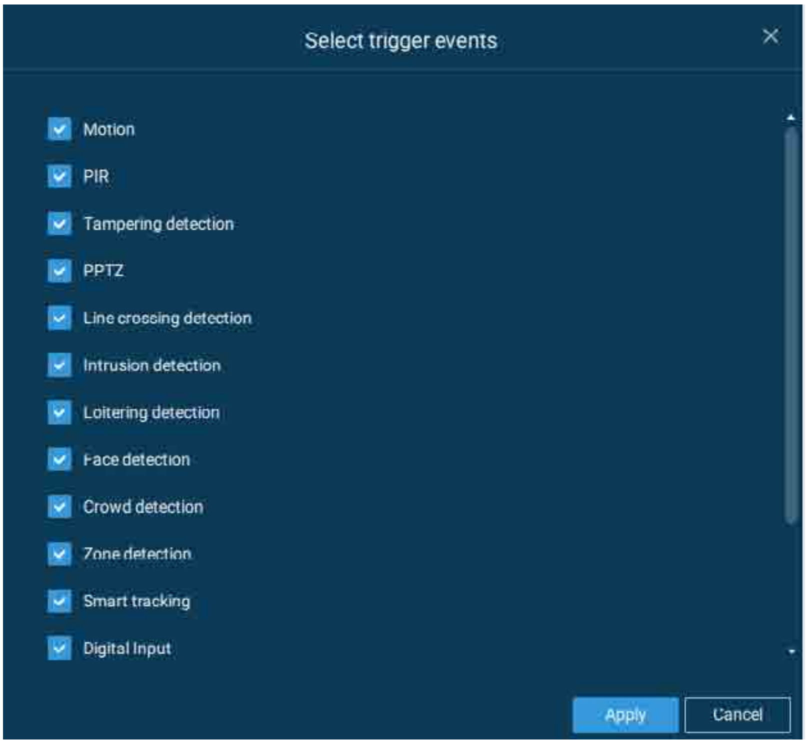
Template name Schedule

00:00~21:30
Events Only

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

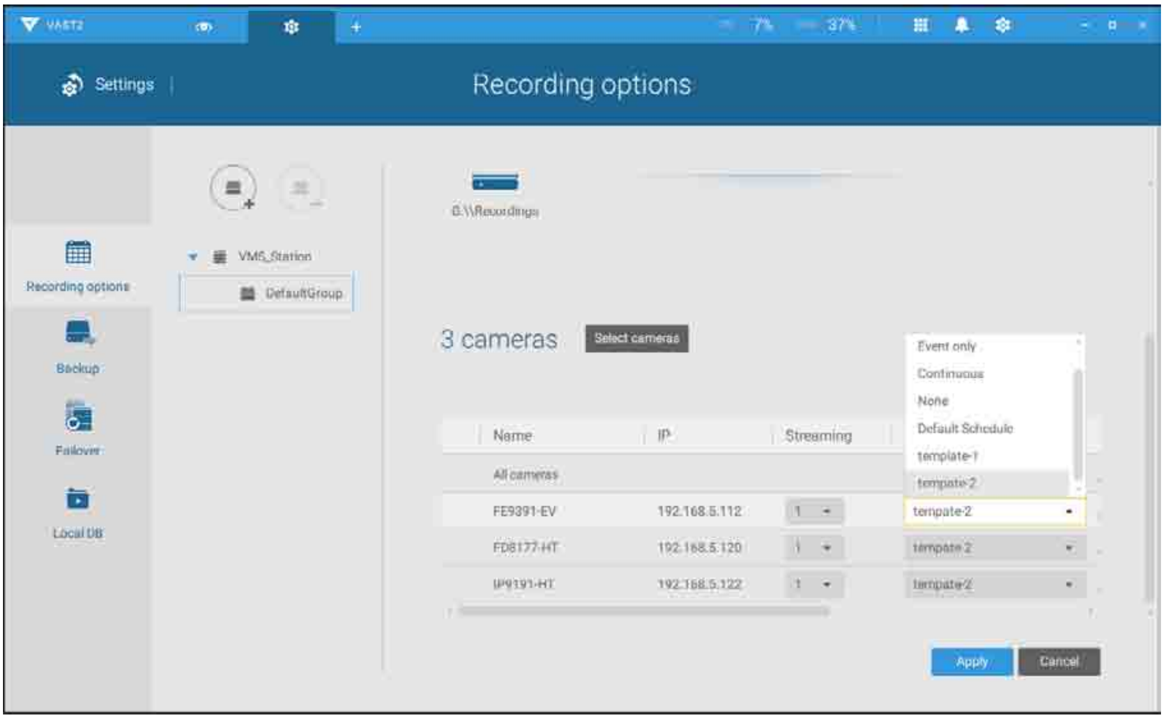


The applicable event types will be listed. Select the types of event triggers that you prefer. Click **Apply** to leave this page. By deault, all applicable event triggers will be selected.


Select trigger events

- ☑ Motion
- ☑ PIR
- ☑ Tampering detection
- ☑ PPTZ
- ☑ Line crossing detection
- ☑ Intrusion detection
- ☑ Loitering detection
- ☑ Face detection
- ☑ Crowd detection
- ☑ Zone detection
- ☑ Smart tracking
- ☑ Digital Input

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.



Settings | Recording options

D:\\Recordings

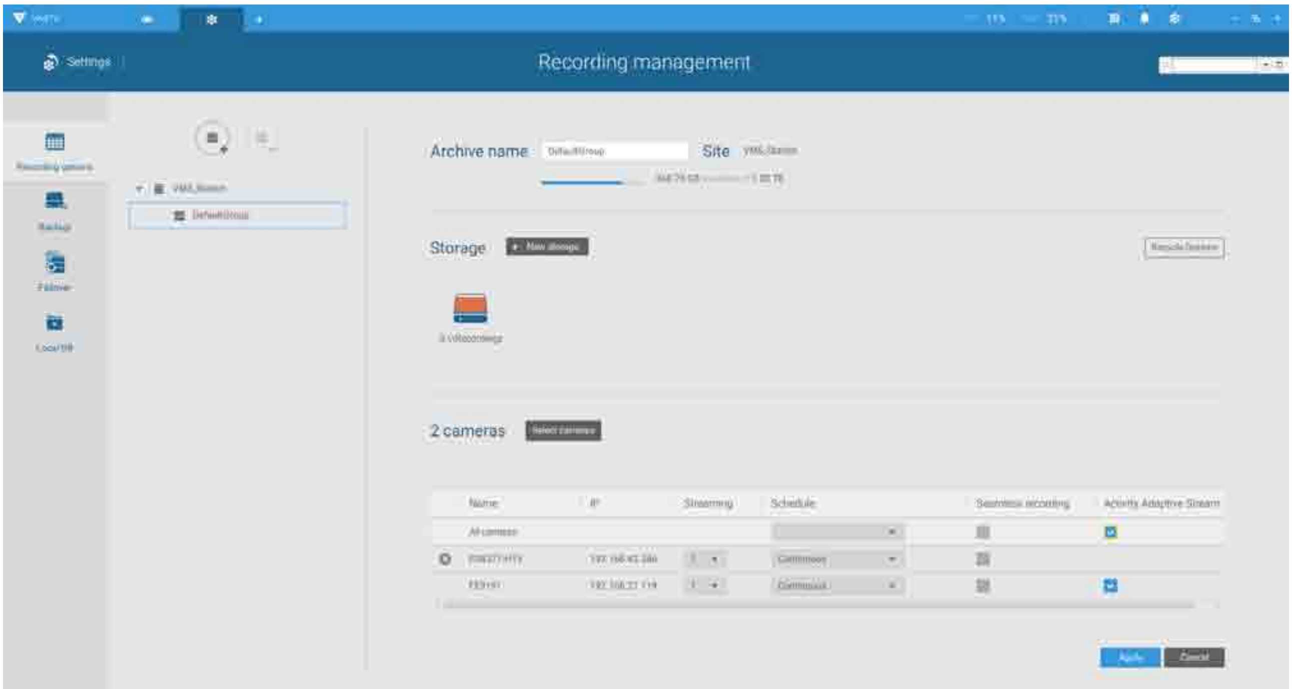
VMS_Station

DefaultGroup

3 cameras Select cameras

Name	IP	Streaming	
All cameras			
FE9391-EV	192.168.5.112	1	tempate-2
FD8177-HT	192.168.5.120	1	tempate-2
IP9191-HT	192.168.5.122	1	tempate-2

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



Settings | Recording management

Archive name DefaultGroup Site VMS_Station

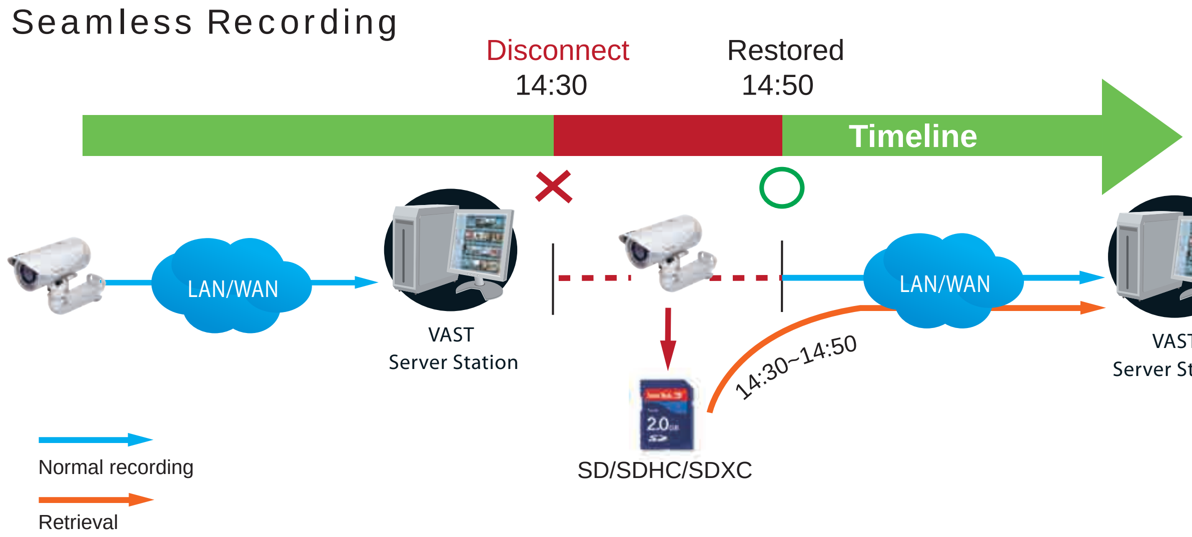
Storage

2 cameras Select cameras

	Name	IP	Streaming	Schedule	Seamless recording	Activity Adaptive Stream
	All cameras					☑
	FD8377-HTV	192.168.45.246	1	Continuous		
	FE9191	192.168.22.119	1	Continuous		☑

Seamless Recording

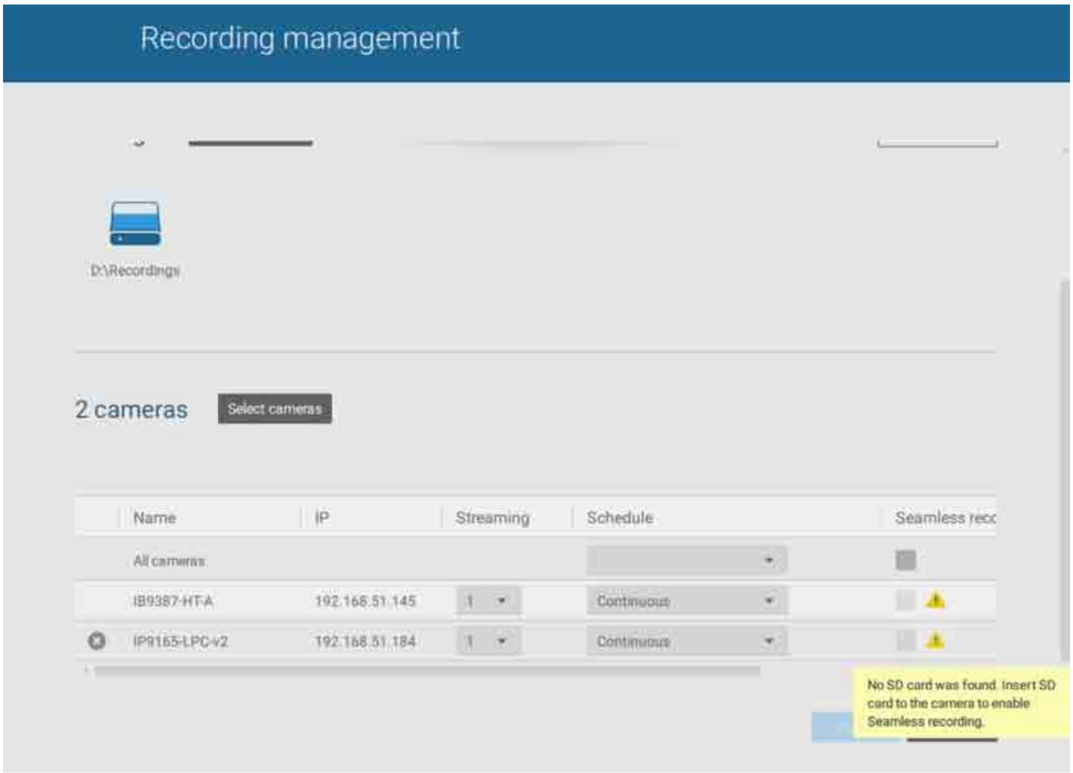
Seamless Recording safeguards critical videos in the occurences of network disconnection. In the event of temporary disconnection, video is stored in individual cameras' SD/SDHC/SDXC card; and once the connection is restored, a VAST server can automatically resume the recording. More remarkable is that,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



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

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

If a camera comes without an SD card, the SD card presence is detected with a warning message.



Recording management

D:\Recordings

2 cameras

	Name	IP	Streaming	Schedule	Seamless recc
	All cameras			▾	■
	IB9387-HT-A	192.168.51.145	1 ▾	Continuous ▾	□ ⚠
⊗	IP9165-LPC-v2	192.168.51.184	1 ▾	Continuous ▾	□ ⚠

No SD card was found. Insert SD card to the camera to enable Seamless recording.

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.

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.

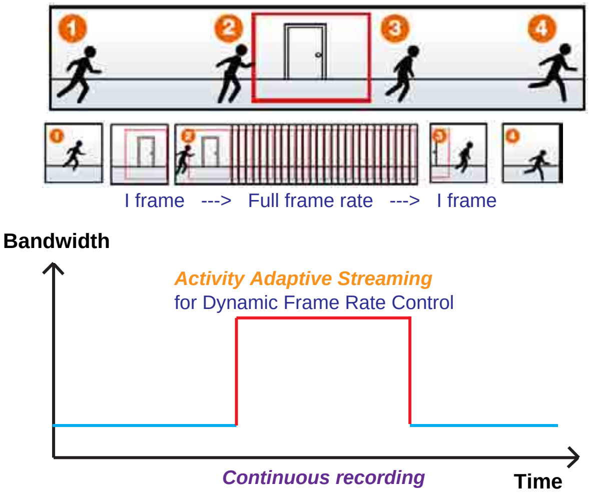
■ Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.

■ 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.


1
2
3
4
I frame ---> Full frame rate ---> I frame
Bandwidth
Activity Adaptive Streaming
for Dynamic Frame Rate Control
Continuous recording
Time

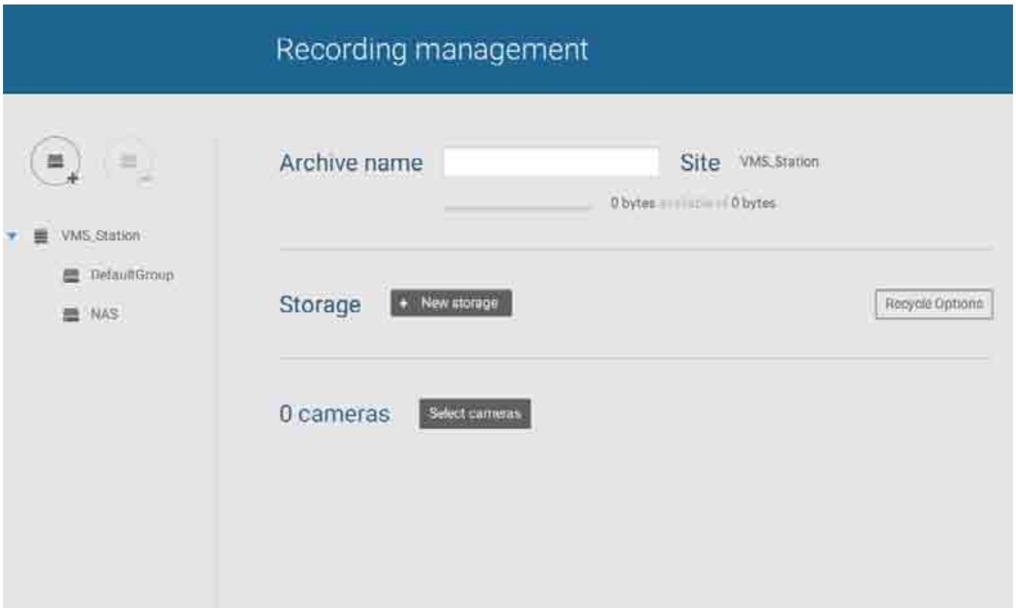
Adding NAS (Network Attached Storage) as a Storage Option

You can also record videos to a networked storage.

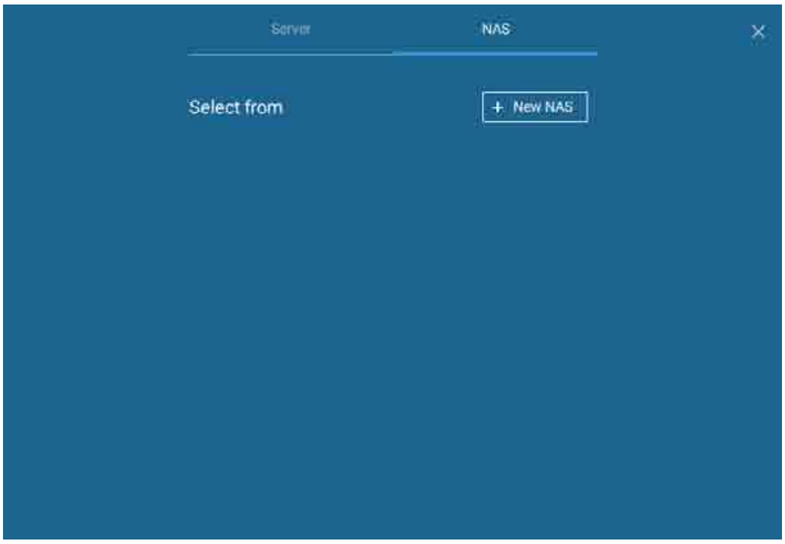
1. Click the Add archive button.

2. Enter a name for the configuration.

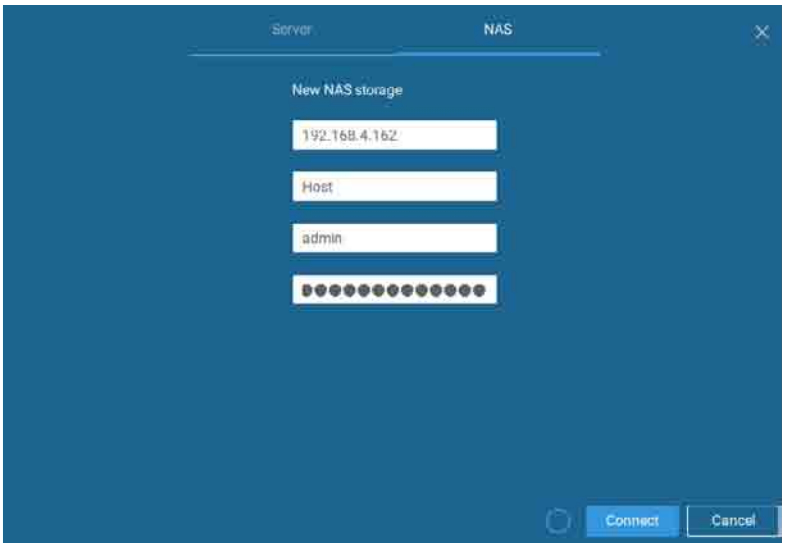
3. Click the Add storage + New storage button.



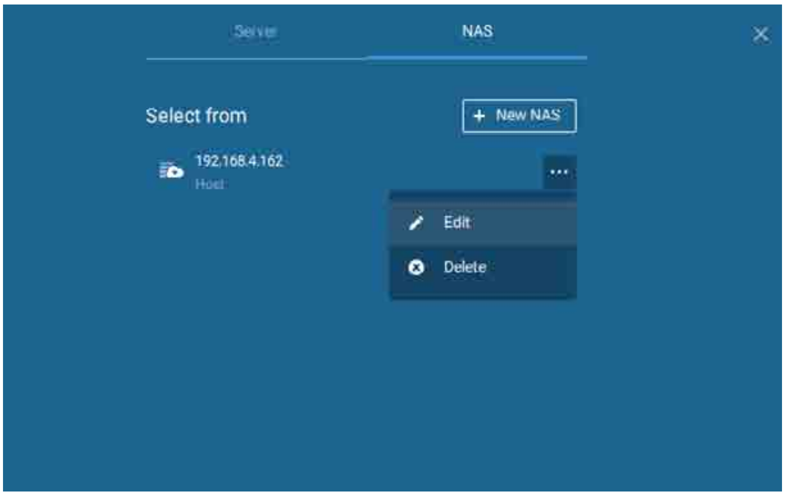
4. Click the + New NAS button.



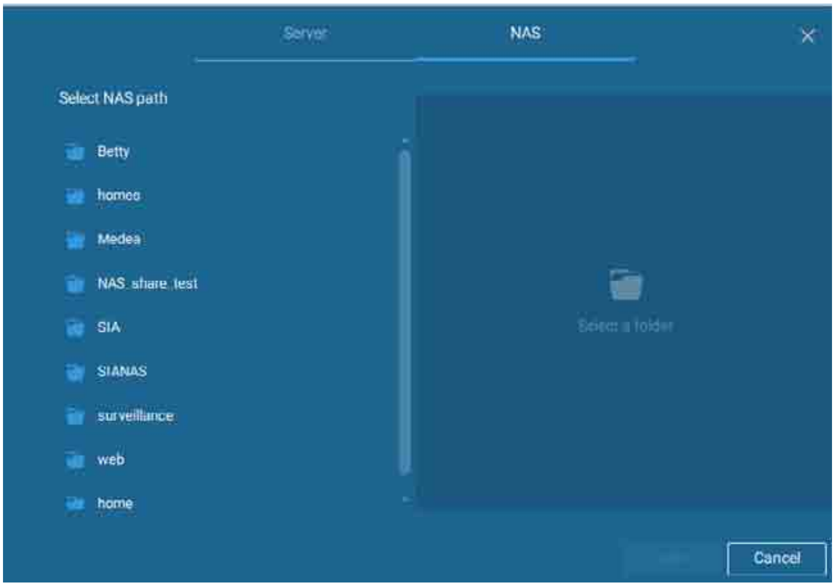
5. Enter the NAS storage's address and the credentials for access to the networked storage. When done, click the **Connect** button.



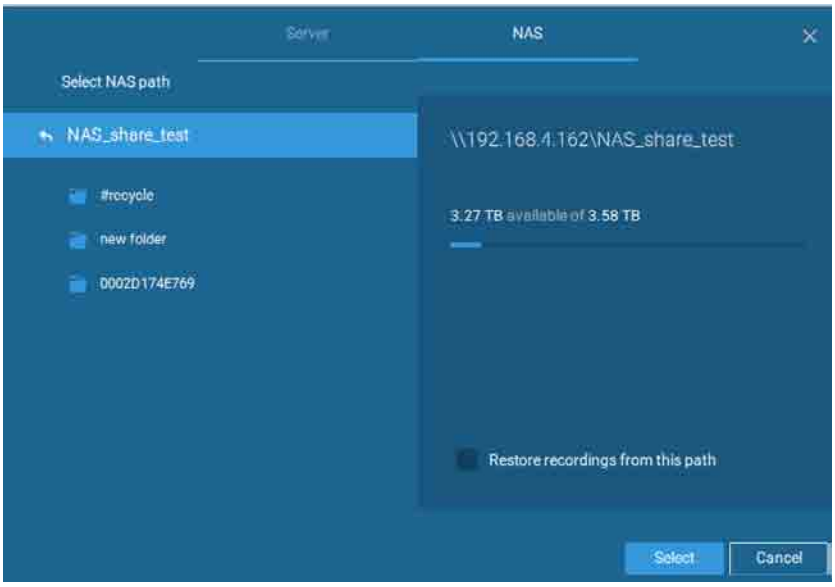
6. The NAS storage should appear on screen. The connection may take several seconds. Single-click on the NAS storage to select its network shares.



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.

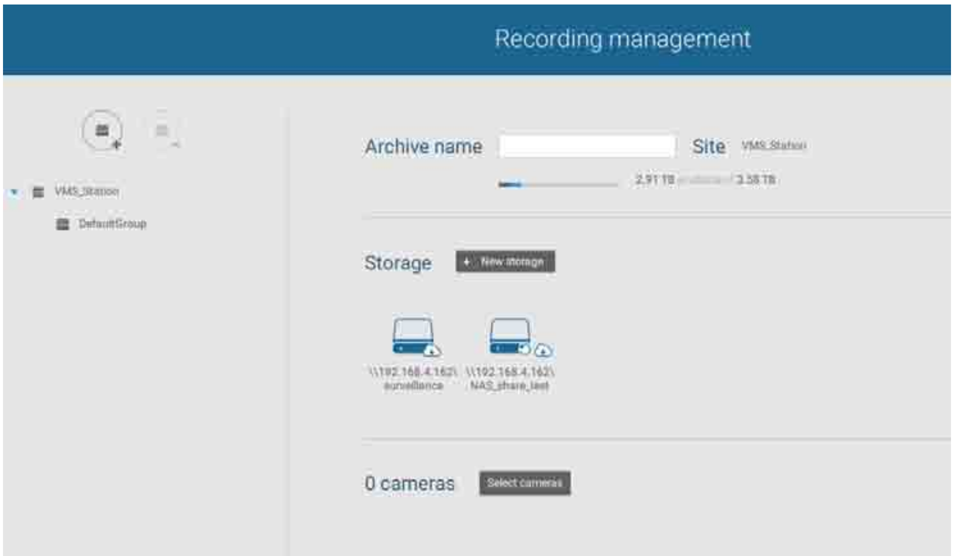


\\192.168.4.162\NAS_share_test

3.27 TB available of 3.58 TB

□ Restore recordings from this path

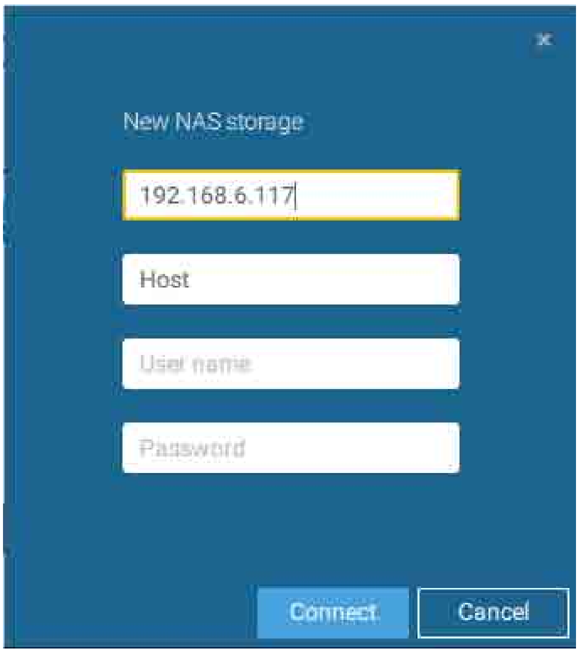
9. The selected shares should be listed. Enter a name and select cameras. When done, click the Add button at the lower right to complete your configuration.



2-3. Storage

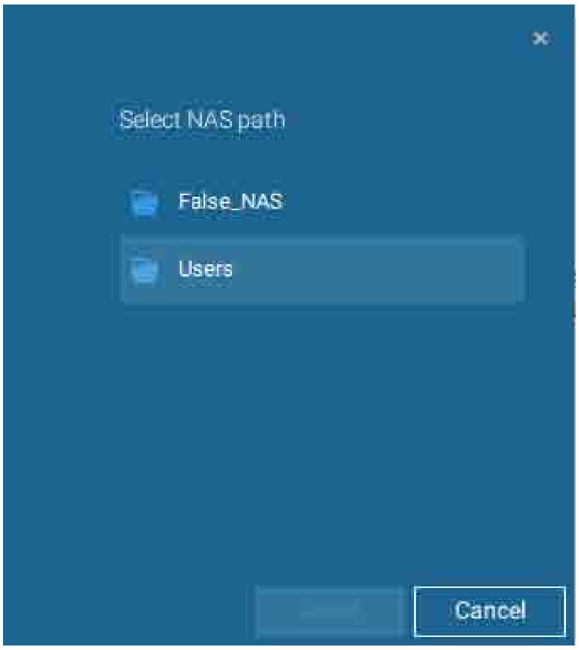
By default, VAST will check if the D: drive is available. If no other disk drives can be specified, the system drive C: will still be defined as a storage option. Other disk drives in the system, and the default storage volume (configured in the initial setup) will be listed.

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



New NAS storage

192.168.6.117



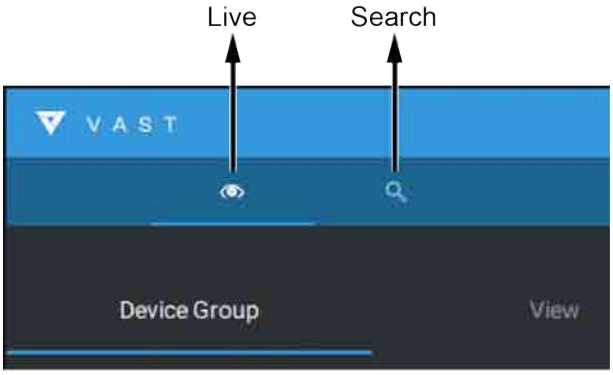
Select NAS path

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 the time settings between them.

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.

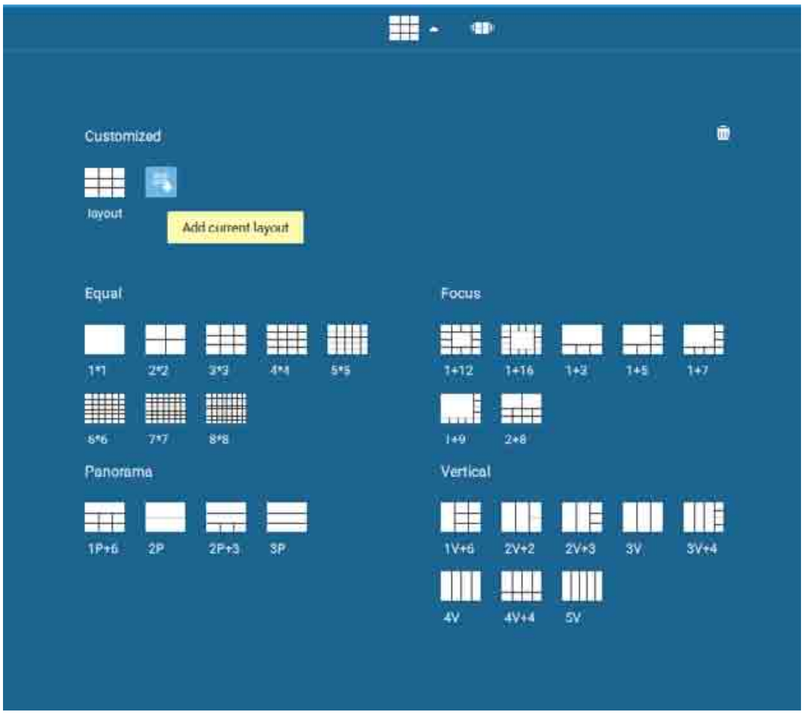
The available layouts are categorized into 4 types: Equal, Panorama, Focus, and Vertical.

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.

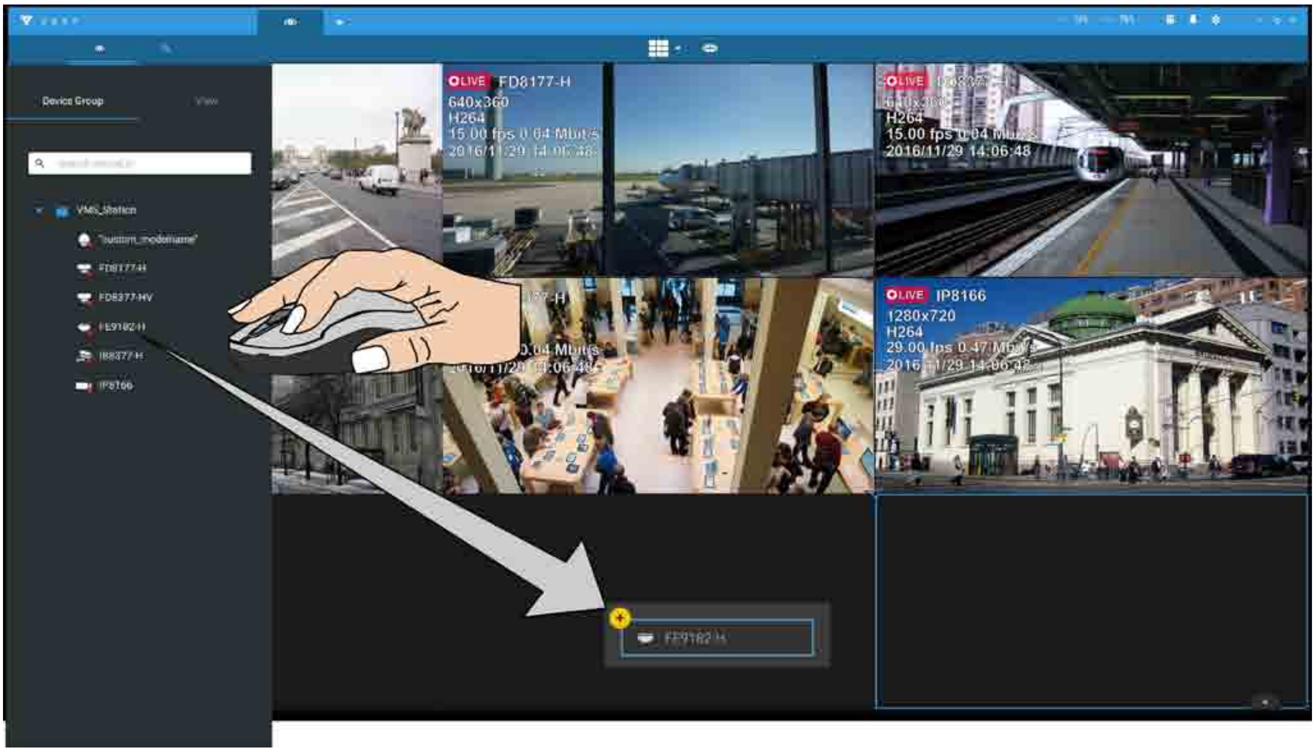
Vertical: 1V+6, 2V+2, 2V+3, 3V, 3V+4, 4V, 4V+4, 5V. (applies to corridor view)



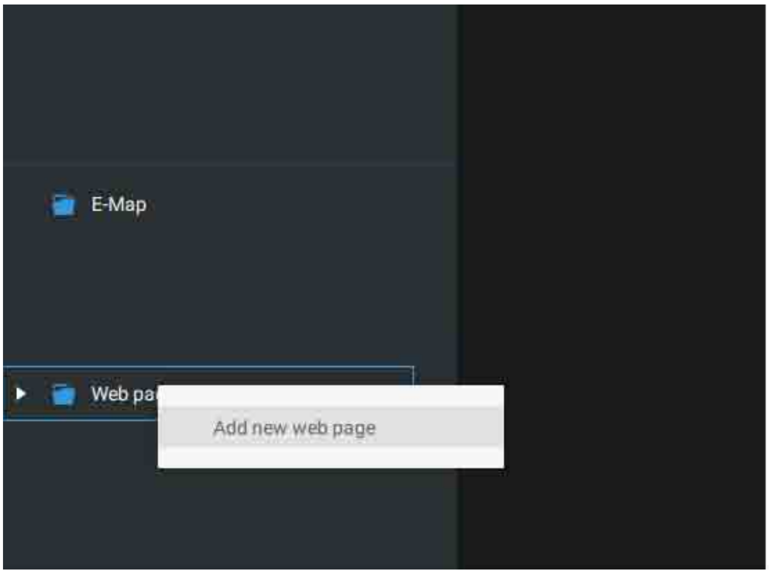
To design and customize a layout, please refer to the Customizable Layout page.

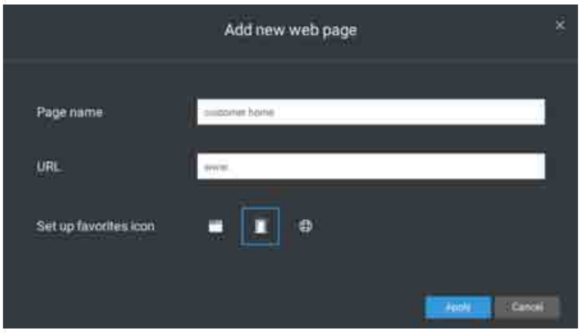
You can then fill in the view cells by dragging and dropping cameras into the view cells. While dragging, a name tag displays. All cameras should be listed under the VMS_Station Device Group.

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



You can also configure a view cell to display a web page by a right-click on the Web page option on the left device pane. Enter a name and the URL address.





Add new web page

Page name: customer home

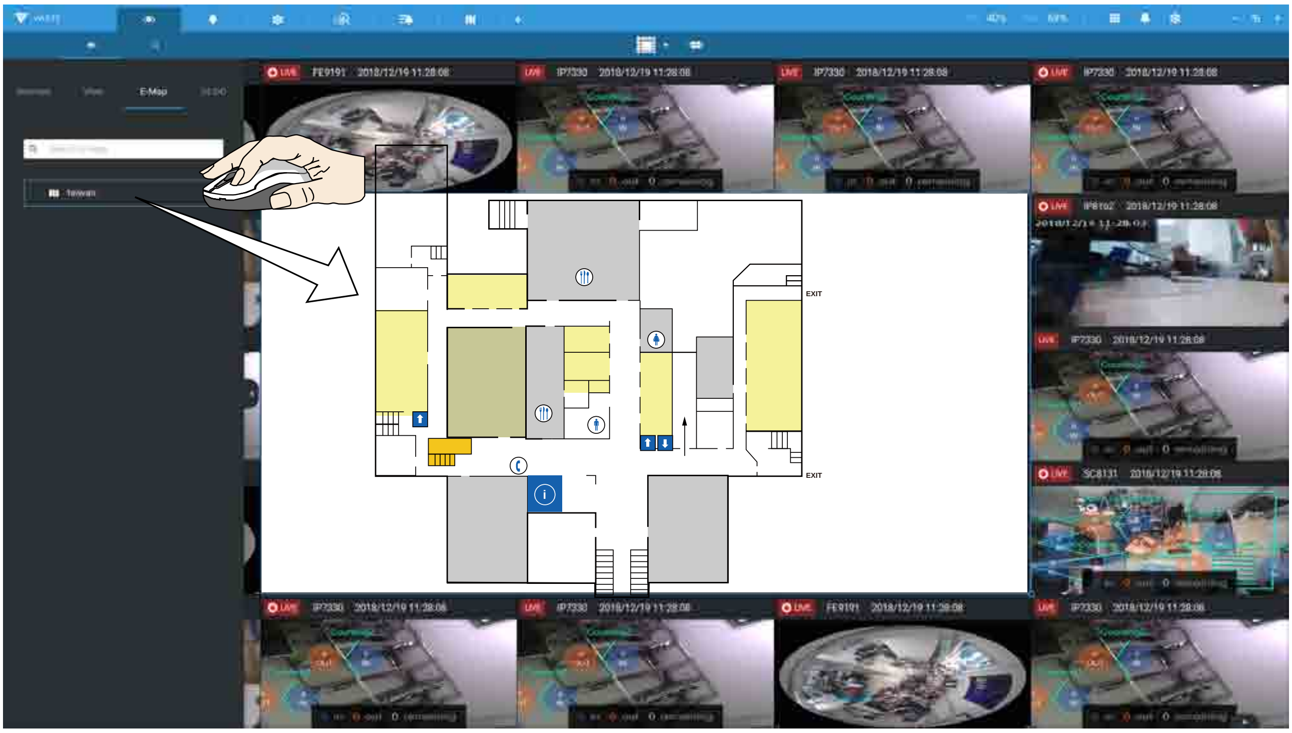
URL: www

Set up favorites icon

When configuring a web page to be displayed in view cell, You can select a favorite icon.

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.

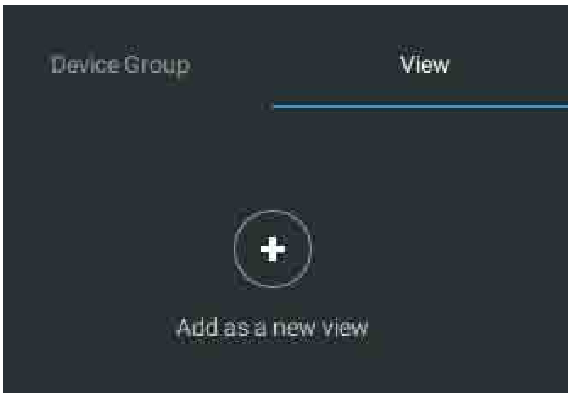
Depending on the resolution of your monitor, a view cell can be too small for an E-Map. For example, for an HD monitor (1920x1080), a single view cell from a 3x3 layout will have a resolution of 640x360. View cells larger than 330 (width) x 300 (height) pixels can contain an E-Map.

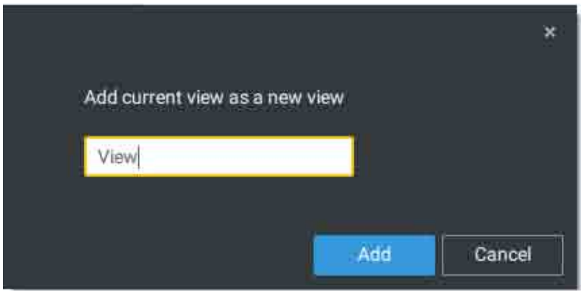

E-Map
LIVE
FE9191 2018/12/19 11:28:08
IP7330 2018/12/19 11:28:08
SC8131 2018/12/19 11:28:08
EXIT
EXIT

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.

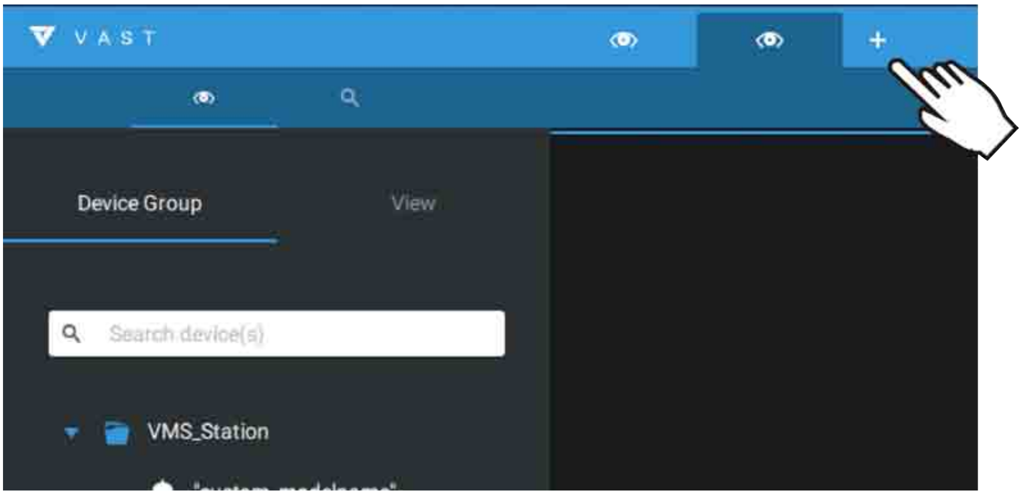




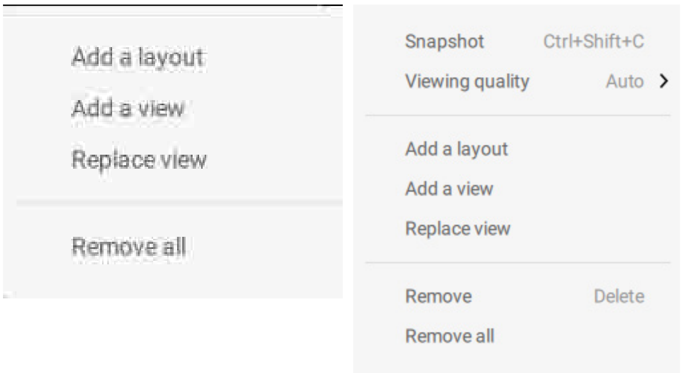
2-6. Add More Live Views

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

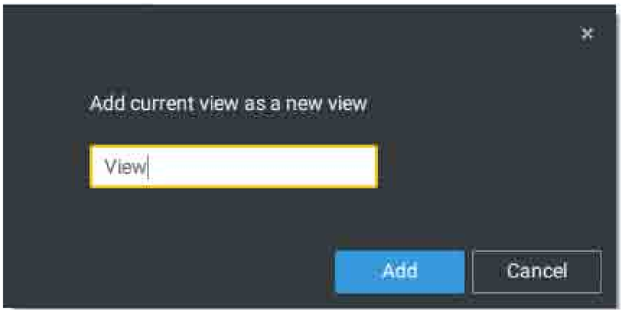
An empty live view will display, and you should repeat the above process to select a layout, and fill in the view cells. When done, save the view.



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

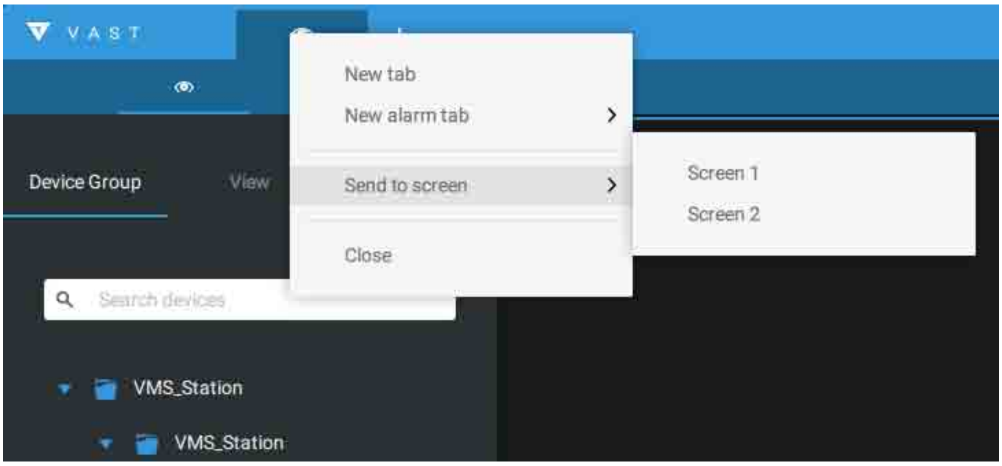


Enter a name for the new view and click **Add** to proceed. The new view will be listed in the View panel.



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.

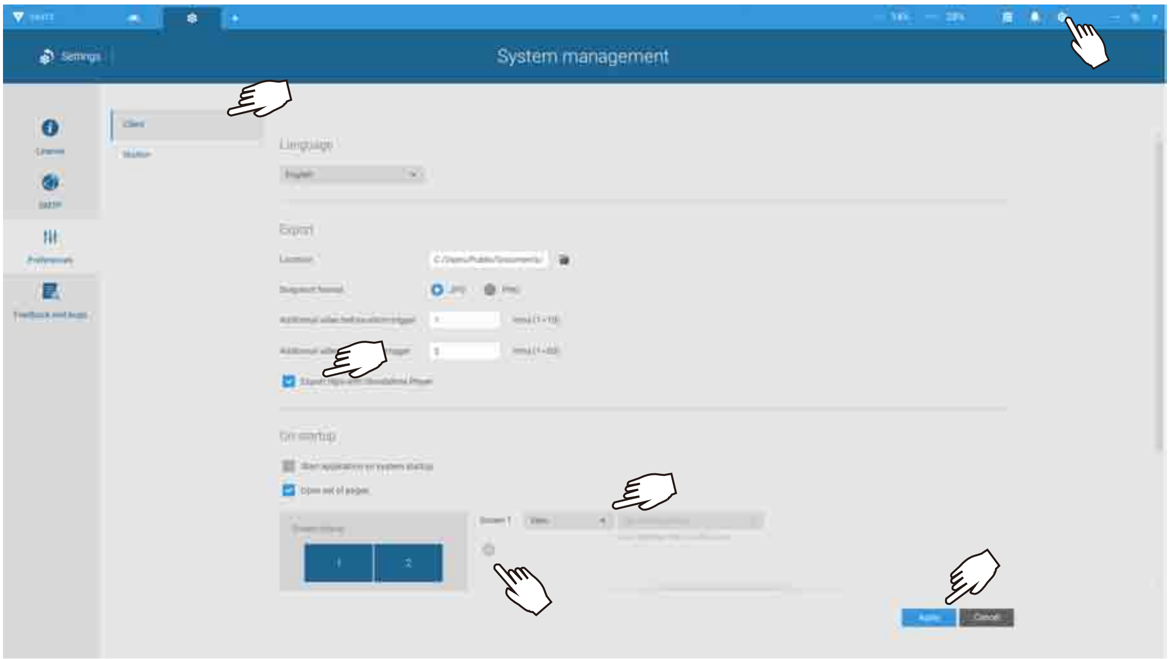
Live views can be placed on multiple monitors. Please note that the number of monitors to display live views is determined by the capability of your system.



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.

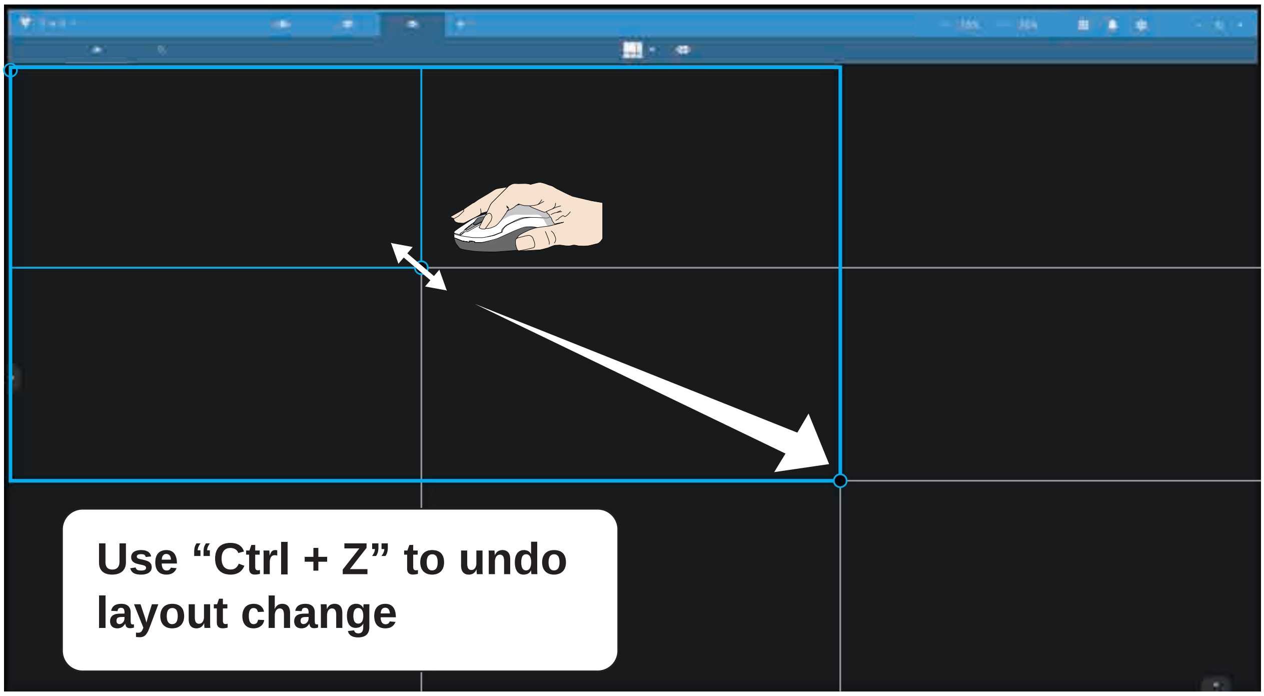


2-8. Customizable Layout

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.

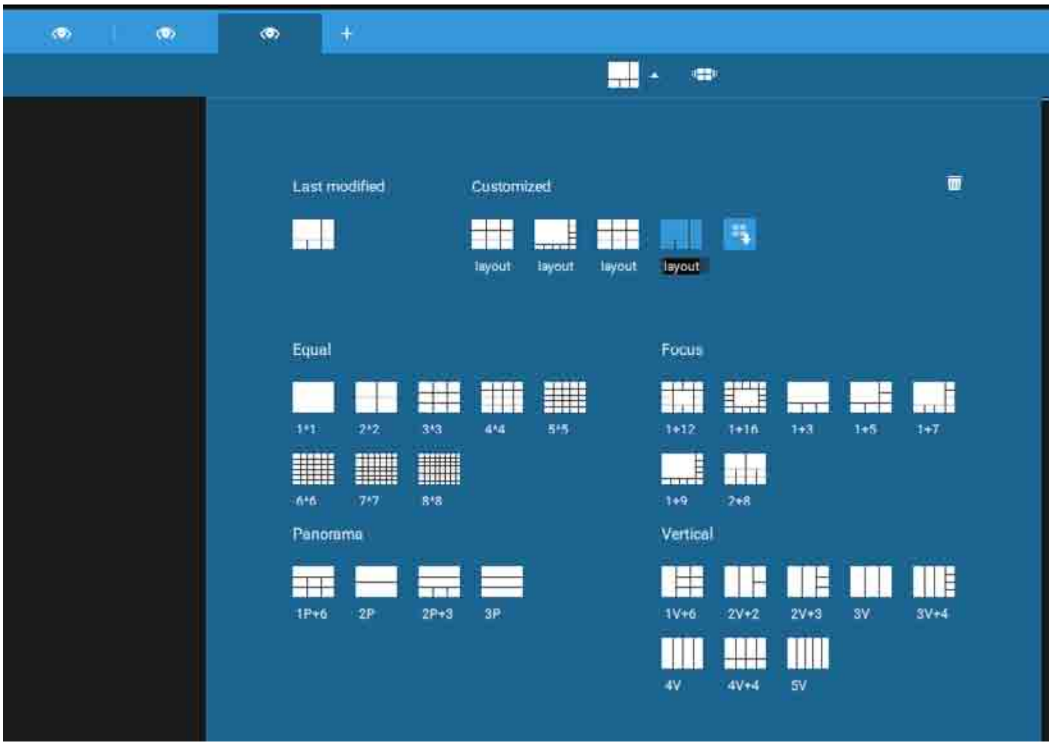
Click and drag the corner mark on a view cell. Drag across the screen and release the mouse button to enlarge the view cell. Choose a standard layout of many view cells, e.g., 7x7 or 8x8, if you want to design a complex customized layout. You can create a special layout, e.g., an especially wide view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

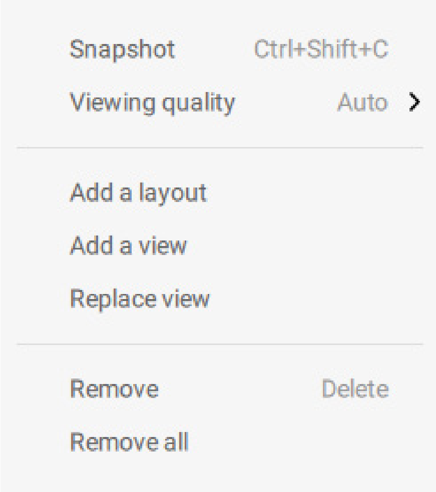
To abandon a customized layout, simply select a new layout from the layout window. You can also use the Ctrl + Z keys to undo your changes on the layout.



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.





Snapshot Ctrl+Shift+C

Viewing quality Auto >

Add a layout

Add a view

Replace view

Remove Delete

Remove all

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

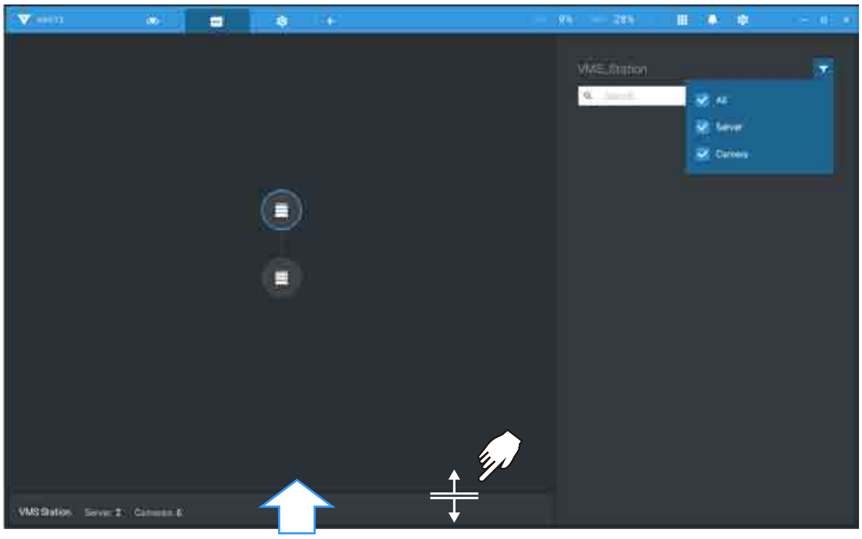
You can then click Device Group, and start filling your customized layout with camera views. When done, click **Add a view**.

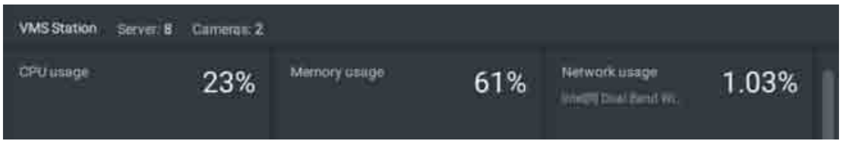
Also remember to save the current layout as a view, and save your configuration in **Settings** > **Preferences**.

2-9. 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.





VMS Station Server: 8 Cameras: 2

CPU usage 23%

Memory usage 61%

Network usage 1.03%

The possible system abnormalities can be:

CPU utilization over 90%

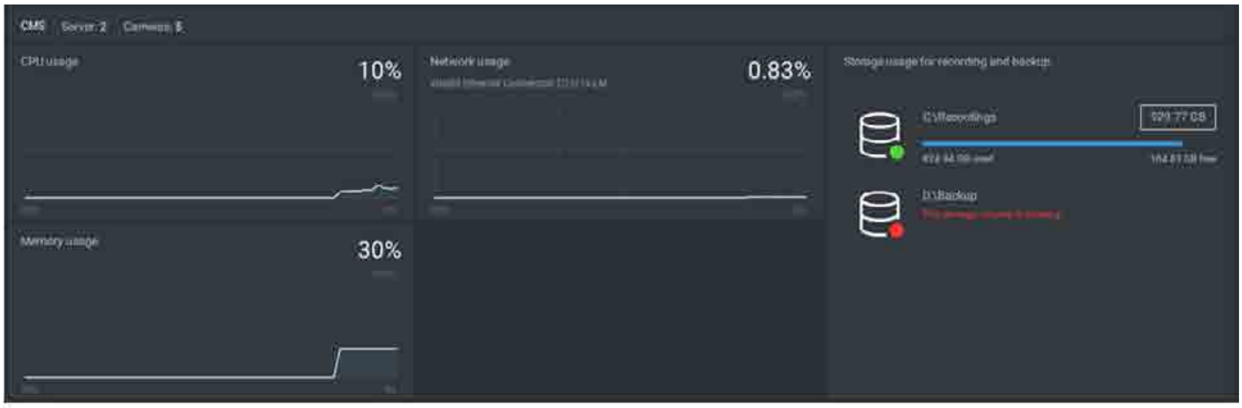
Memory usage over 90%

Network usage over 90%

Camera disconnected

Station disconnected

If you have multiple LAN cards or virtual HBAs, the status row can be pulled to reveal all of their statuses. The storage volume status is also displayed in terms of recording and backup with the total, used, available size displayed. If a volume went down or is disconnected, notifications will appear on the status panel.



CMS Server: 2 Cameras: 5

CPU usage 10%

Network usage 0.83%

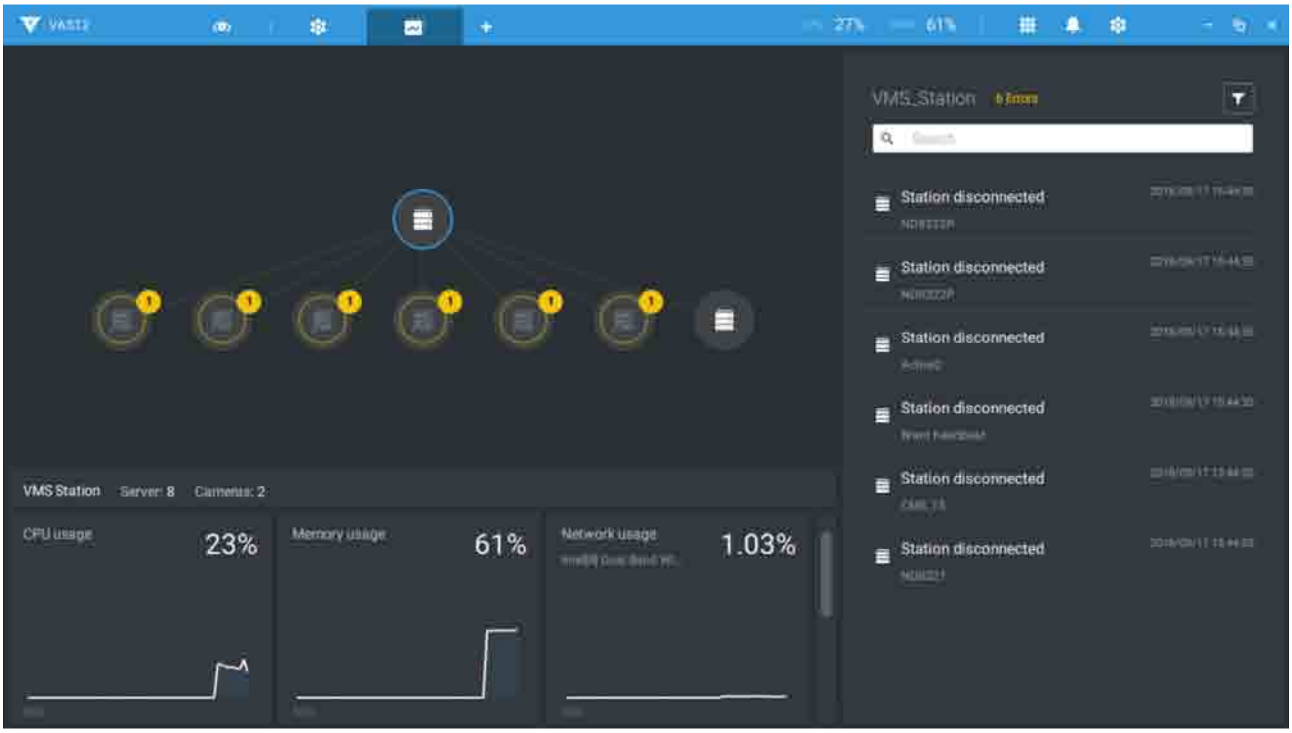
Storage usage for recording and backup

C:\Recordings

D:\Backup

Memory usage 30%

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



VMS_Station 6 Errors

Station disconnected
ND8322P

Station disconnected
ND9322P

Station disconnected
[illegible]

Station disconnected
[illegible]

Station disconnected
[illegible]

Station disconnected
ND9321

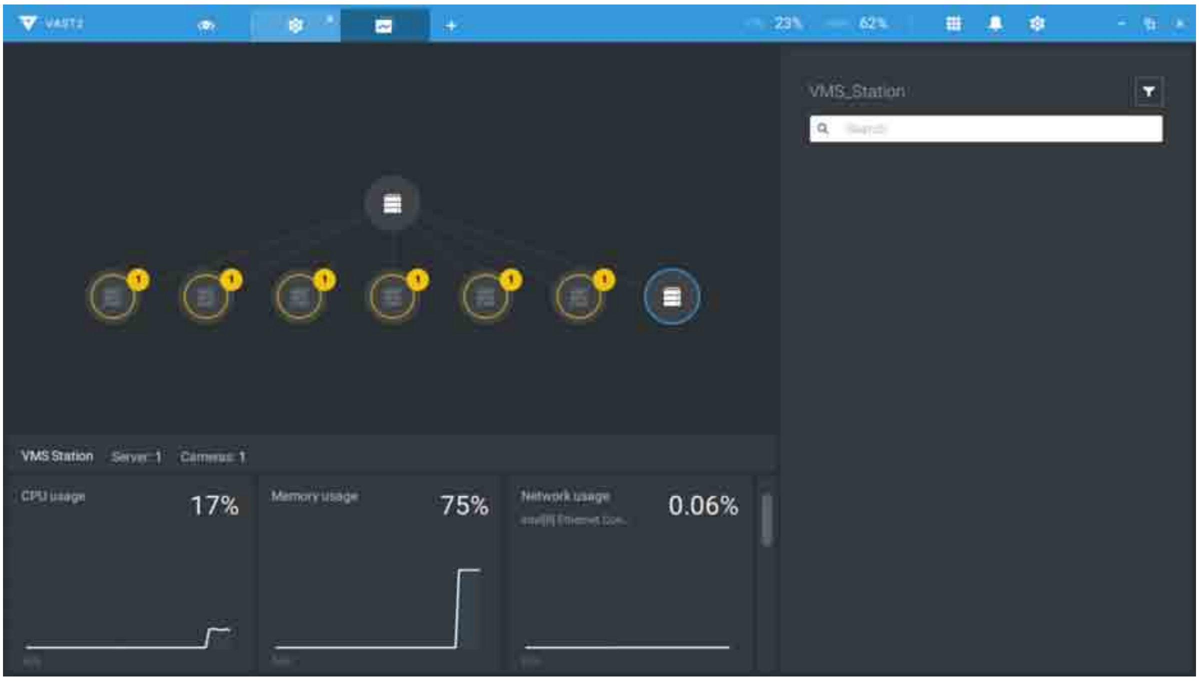
VMS Station Server: 8 Cameras: 2

CPU usage 23%

Memory usage 61%

Network usage 1.03%

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



VMS_Station

VMS Station Server: 1 Cameras: 1

CPU usage 17%

Memory usage 75%

Network usage 0.06%

2-10. E-Map

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

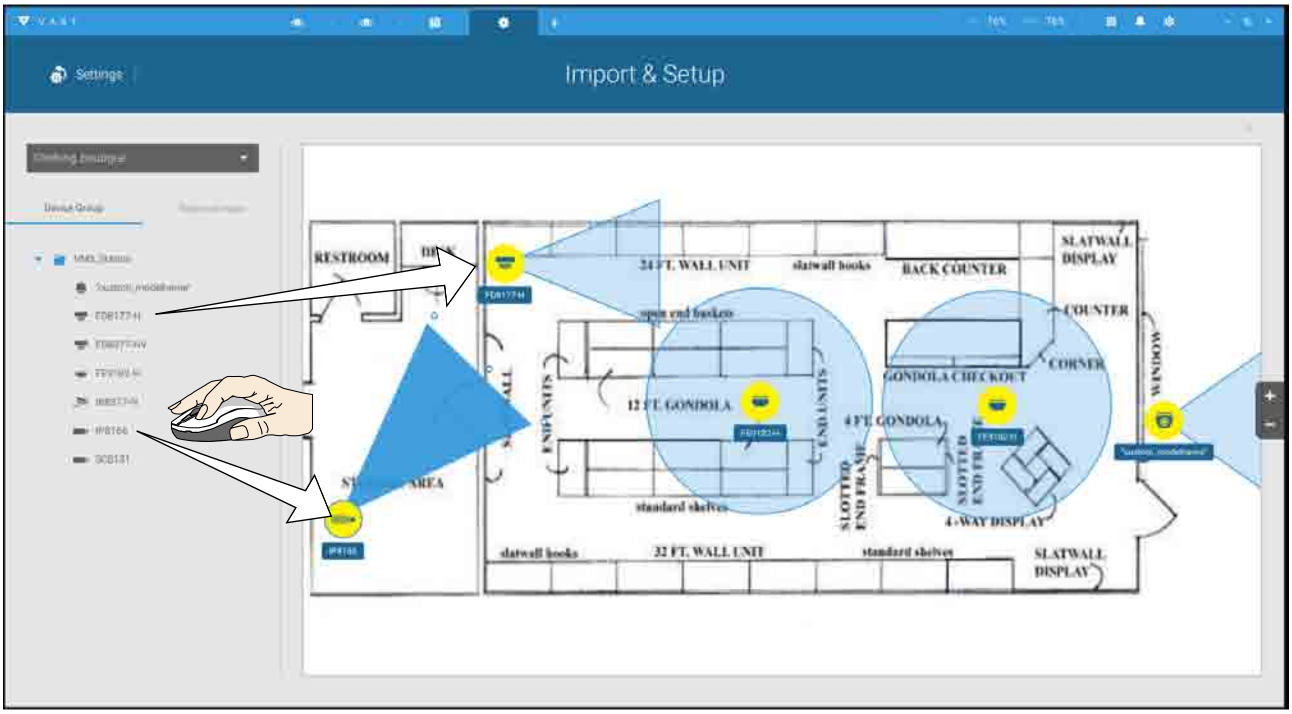
E-Map

Import & Setup

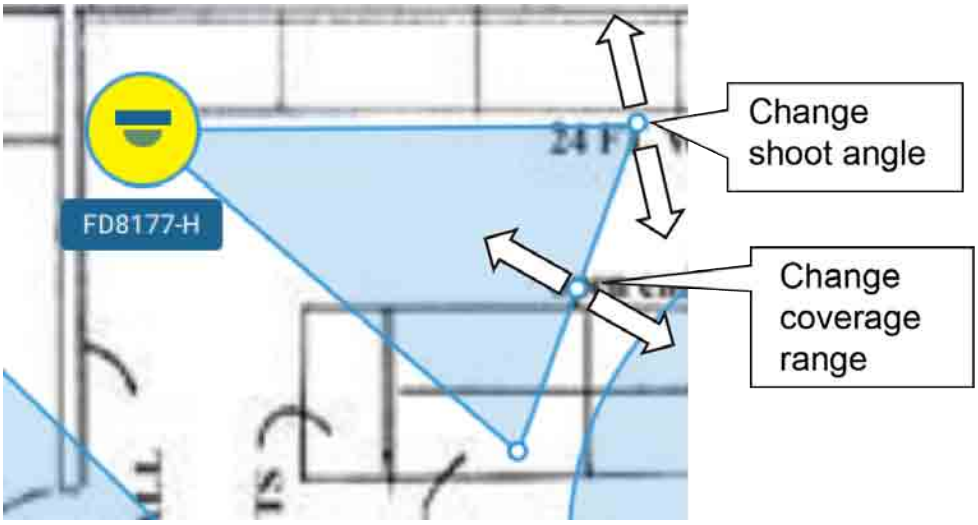
Click Import file ▣ or Import folder ▣. An entire folder can be imported.

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

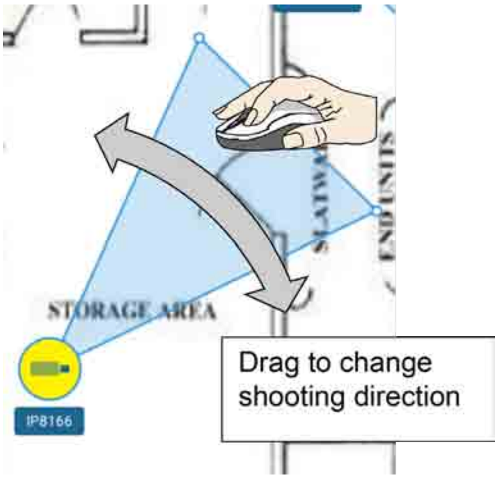
Your cameras will be listed on the left. Drag and drop the cameras to the corresponding locations on the map.



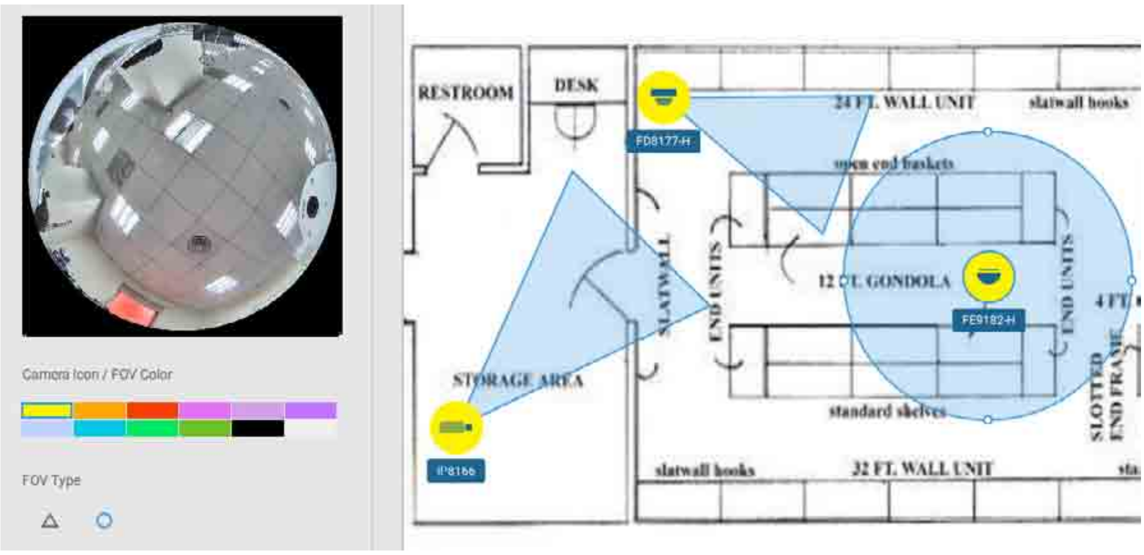
When the camera is in place, drag the FOV indicators on the edge to change the shooting angle and the coverage range.



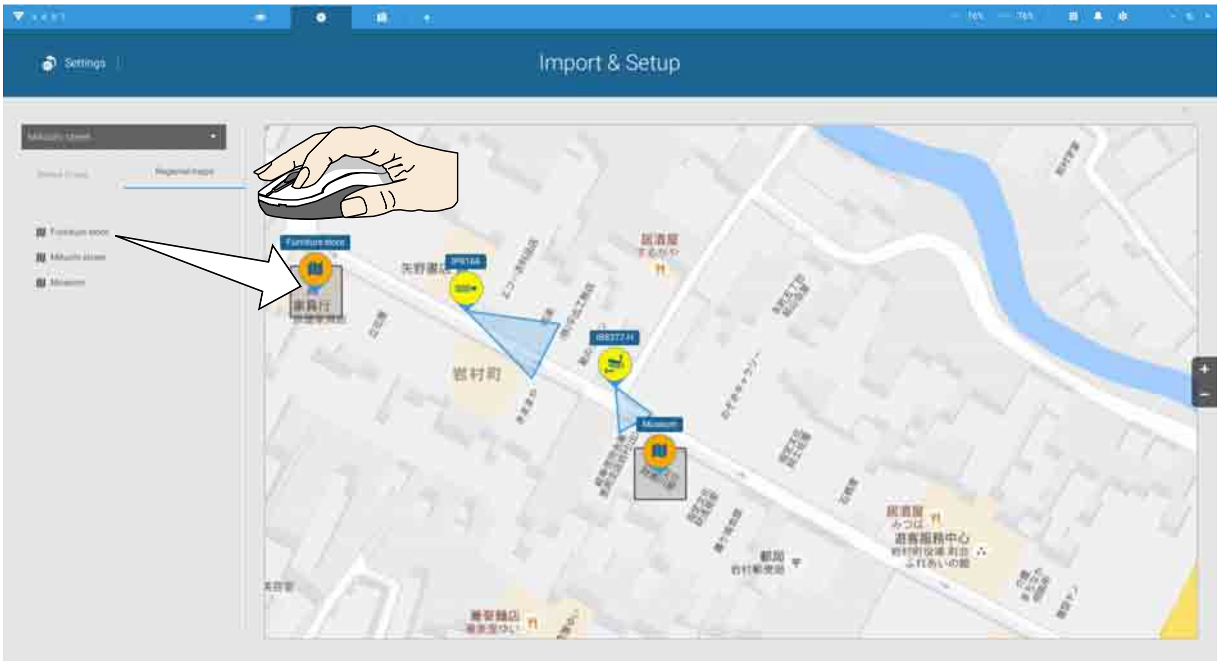
Drag the FOV to change the shooting direction to match the actual installation.



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.

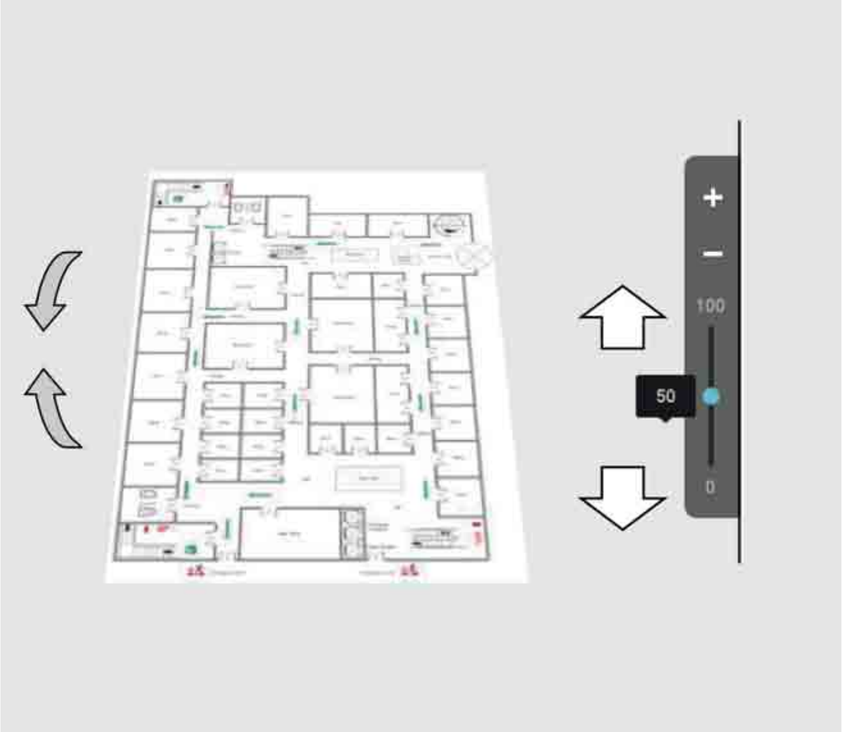


If you have a larger regional map that covers a geographical area, say, a street block, you can drag one or many E-Maps into it. For example, you can place another E-Map that is used to indicate the camera deployment inside a building that is located on the street.



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.



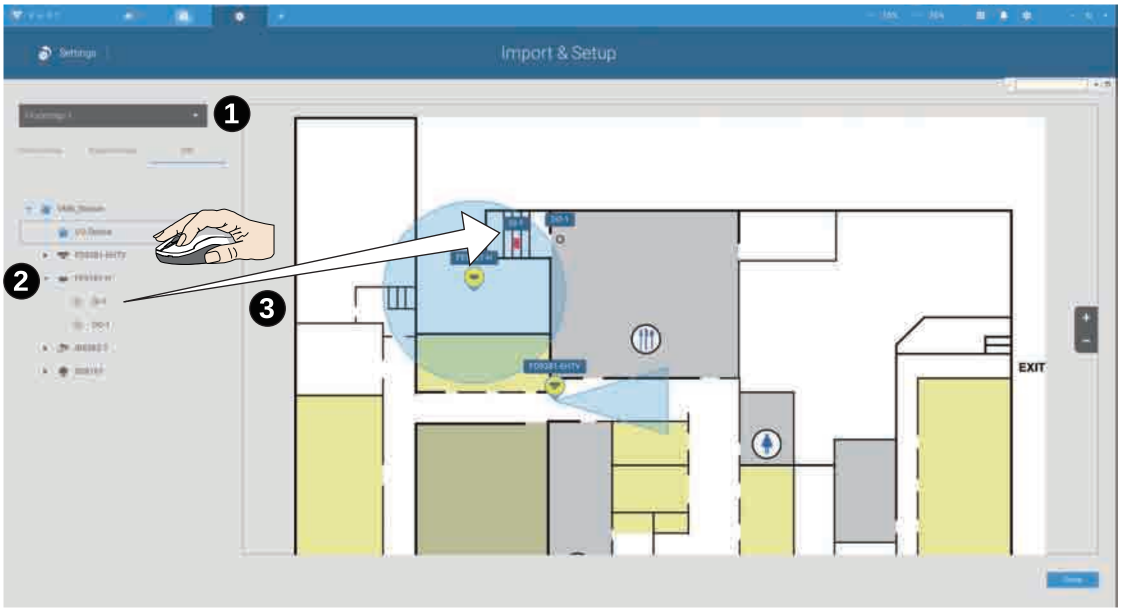
Placing DI/DO Devices

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.

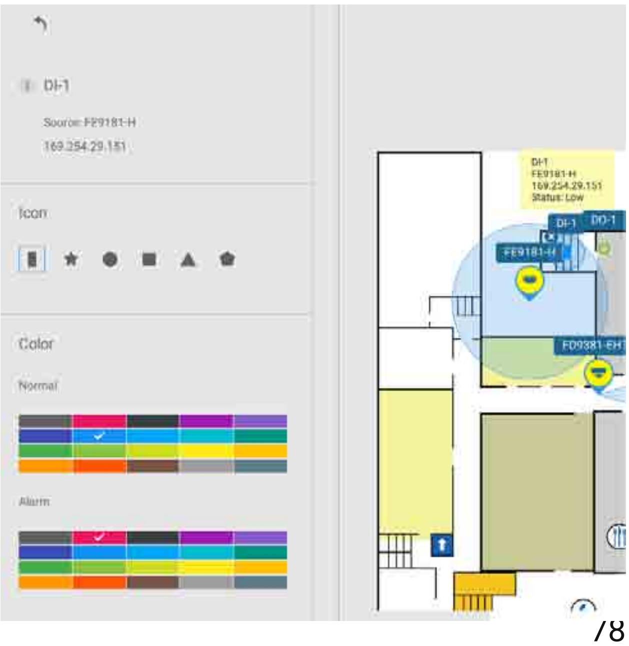
2. Unfold the sub-trees beneath the network camera, (taking camera DI/DO devices as an example).

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.



DI-1

Source: FE9181-H

169.254.29.151

Icon

Color

Normal

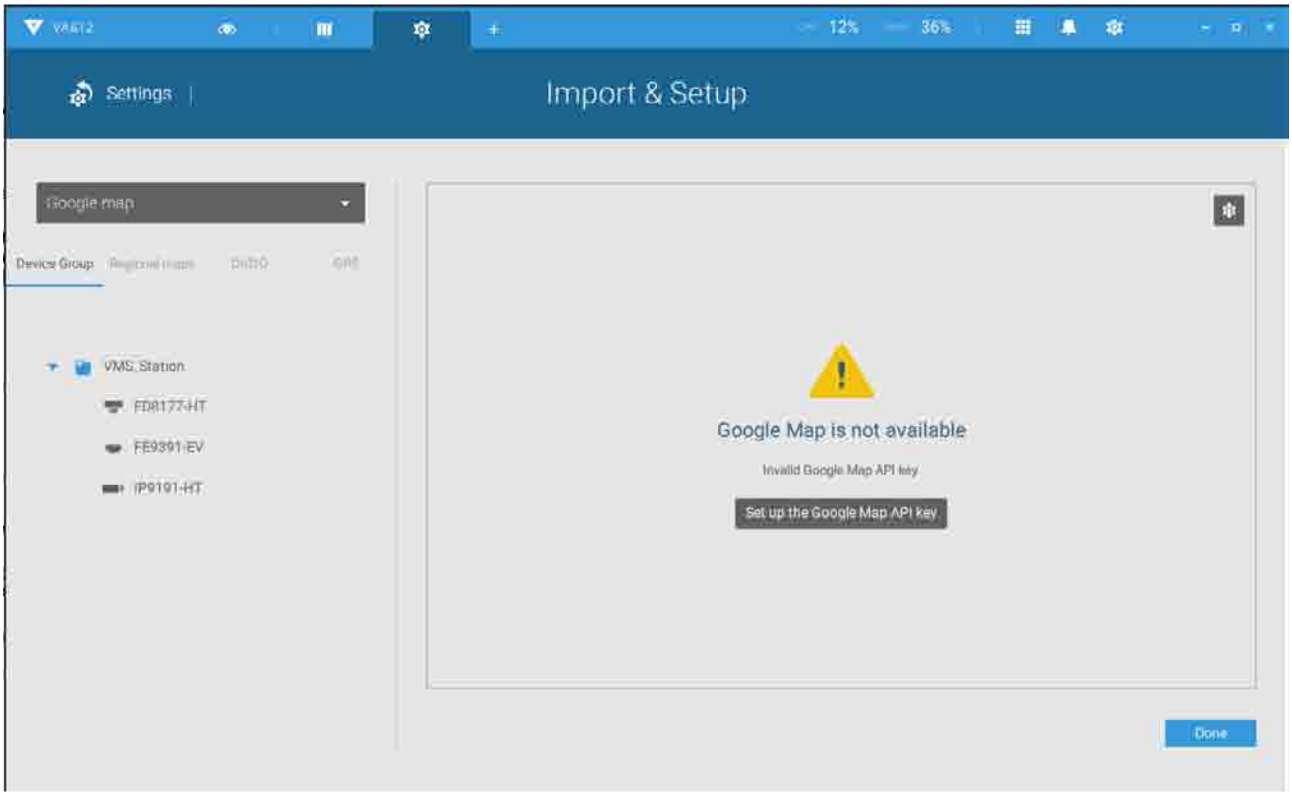
Alarm

Configuring GIS or 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/

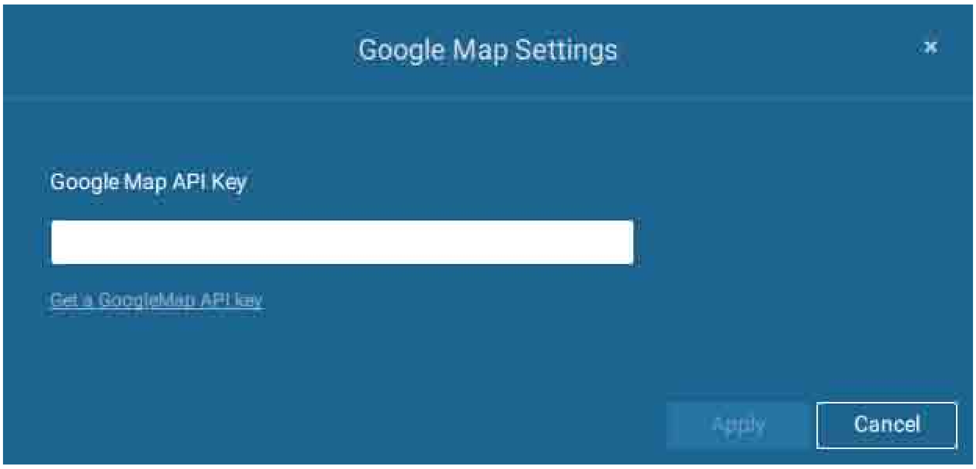
Visit Settings > Emap > All Maps.



Google Map is not available

Invalid Google Map API key

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

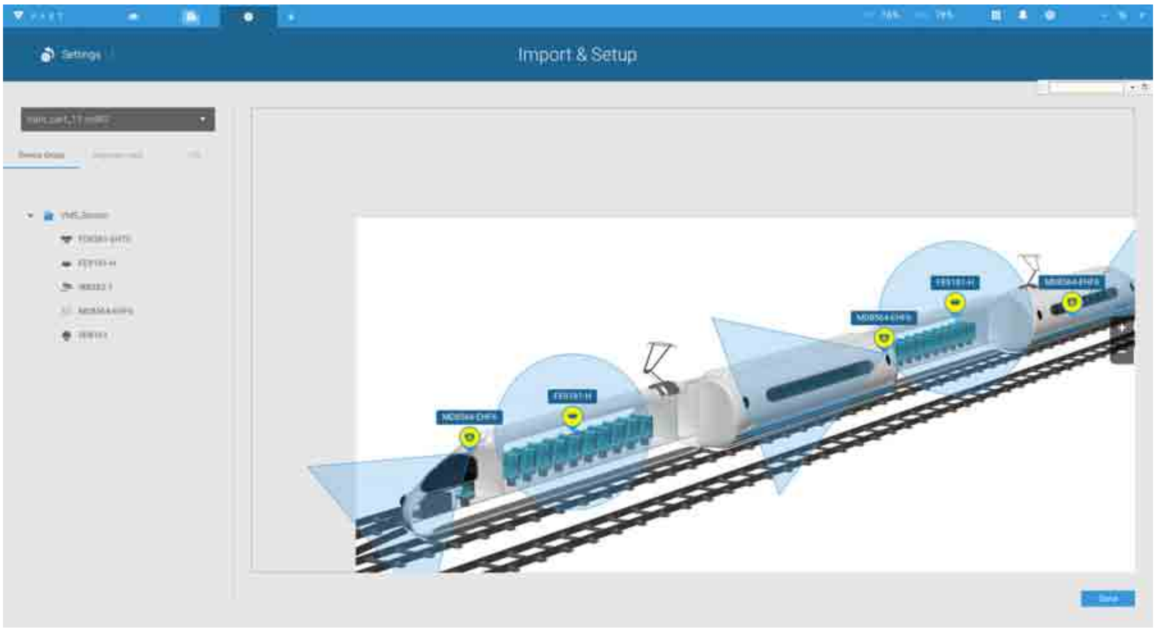


Google Map API Key

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.

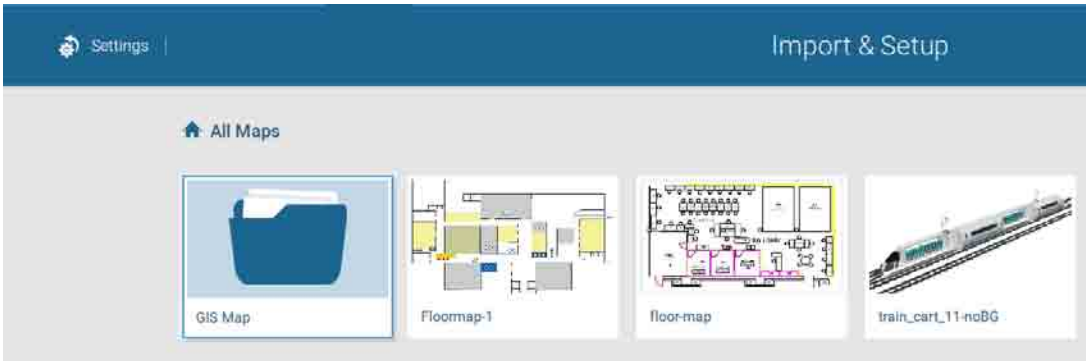
Before configuration on a Google Map, you should prepare an E-map drawing for special installations, such as that on a vehicle. The vehicle, e.g., a train, should come with a GPS-GSM/GPRS module to collect the position information and pass this information to a web-server. As new data is constantly inserted 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 functionality.

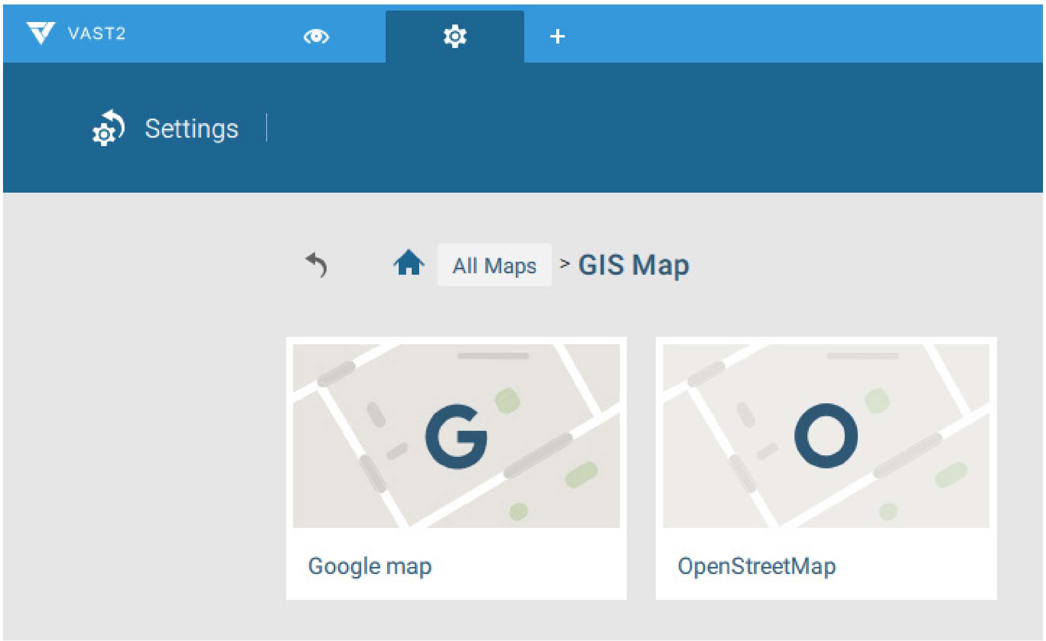


Open the E-Map Import & Setup window.

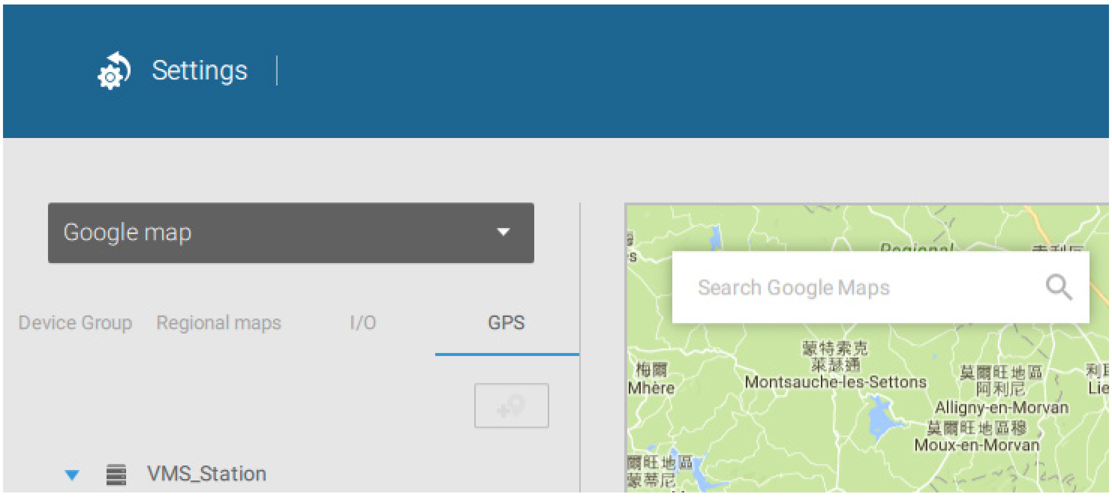
Click to enter the GIS (Geographic Information System) Map and then Google Map window.



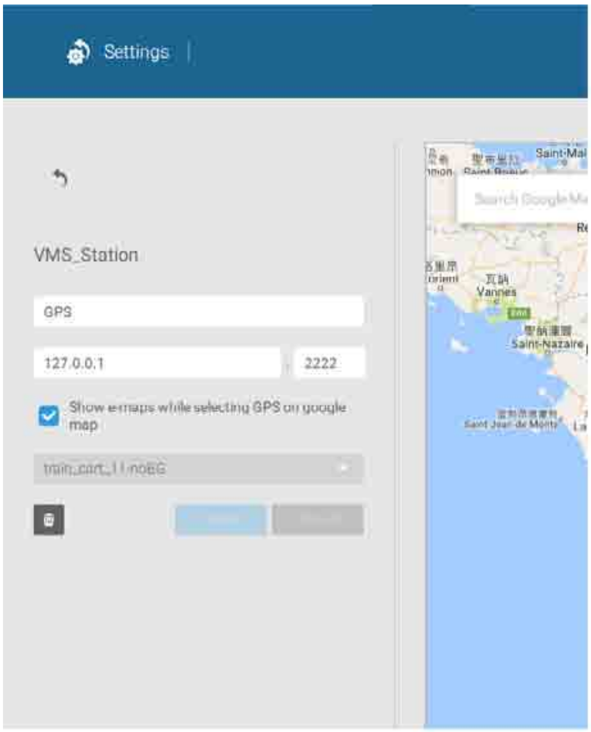
Click on either the Google map or the OpenStreetMap.



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



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



VMS_Station

GPS

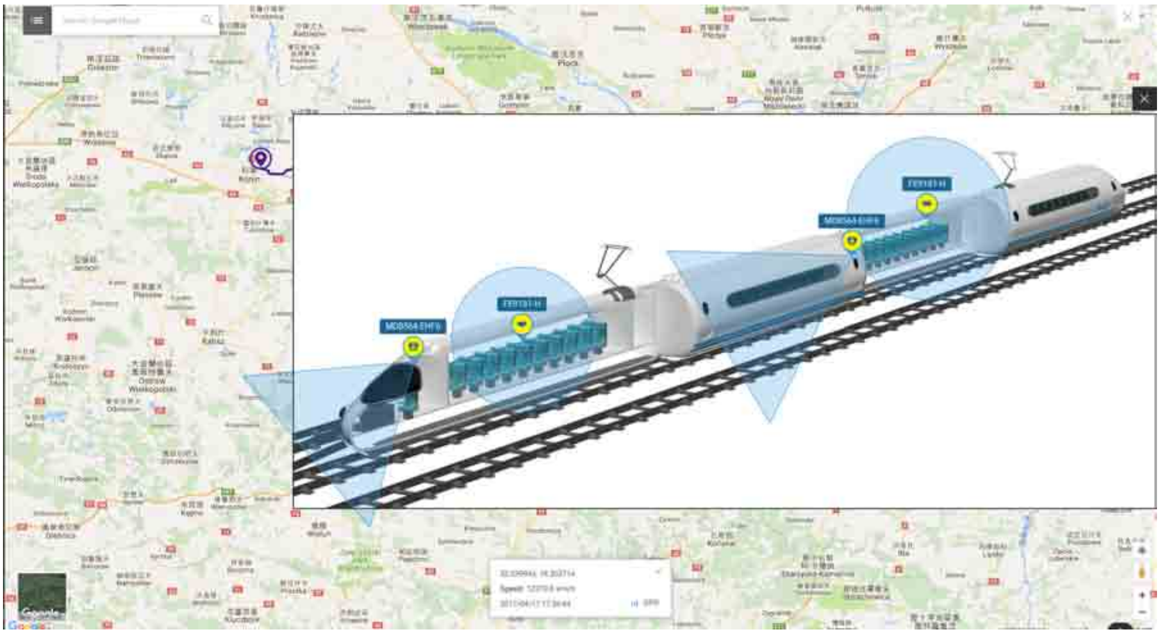
127.0.0.1 : 2222

☑ Show e-maps while selecting GPS on google map

train_cart_11noBG

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.

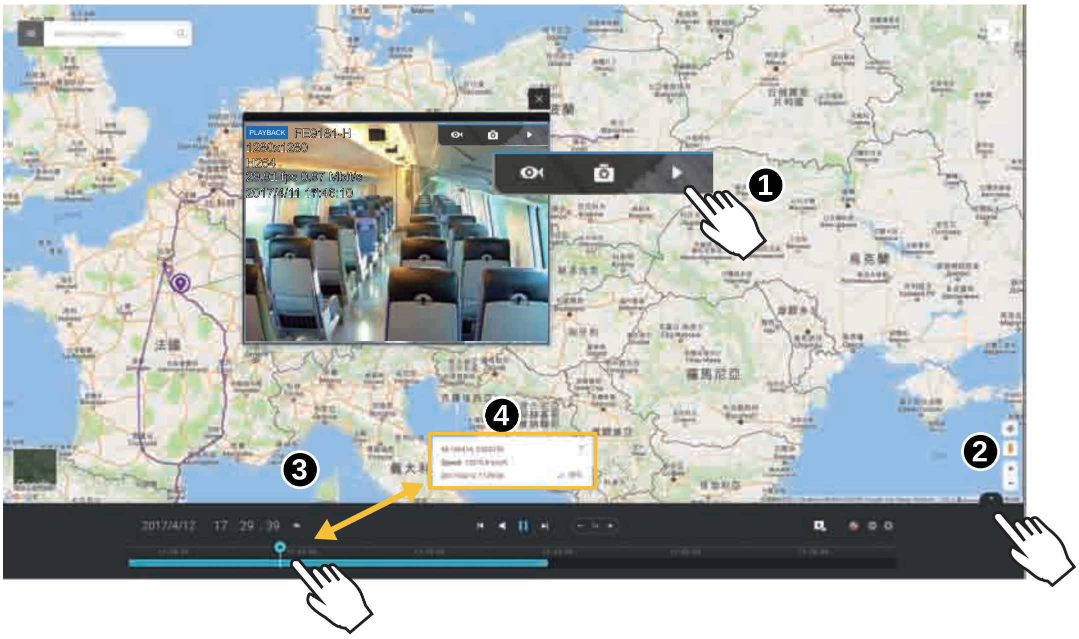
To search and review recordings when an event occurs,

1. Click on the Playback button.

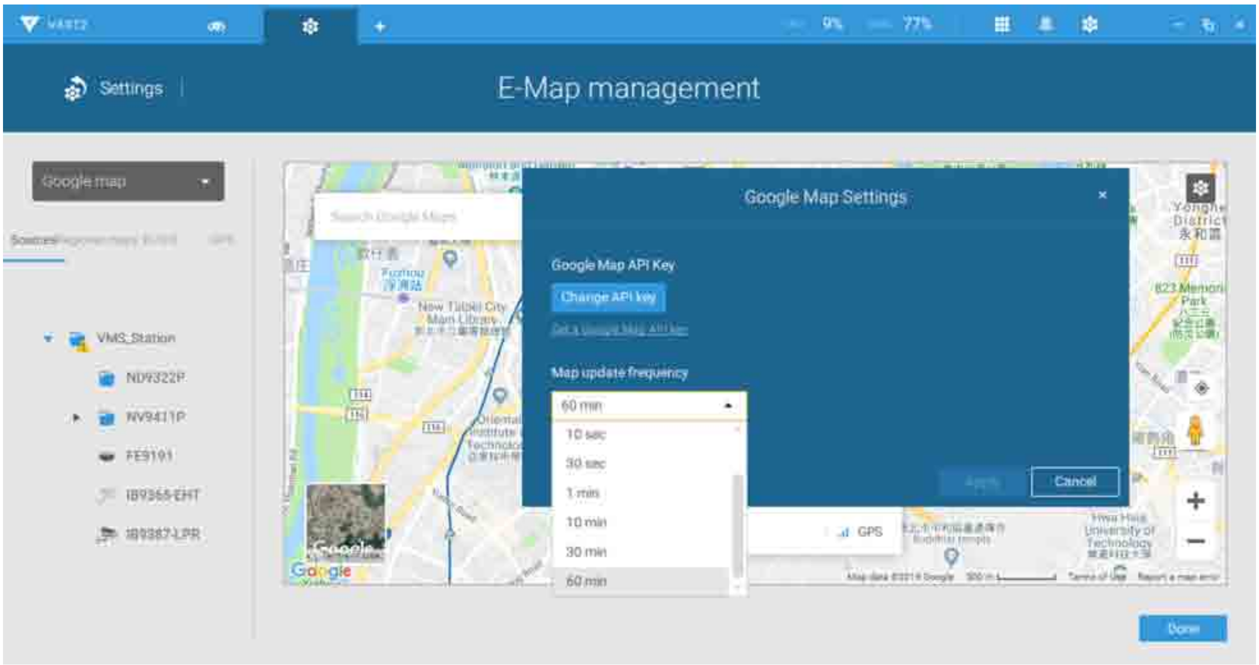
2. Click the Pane button to display the Playback control panel.

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.



E-Map management

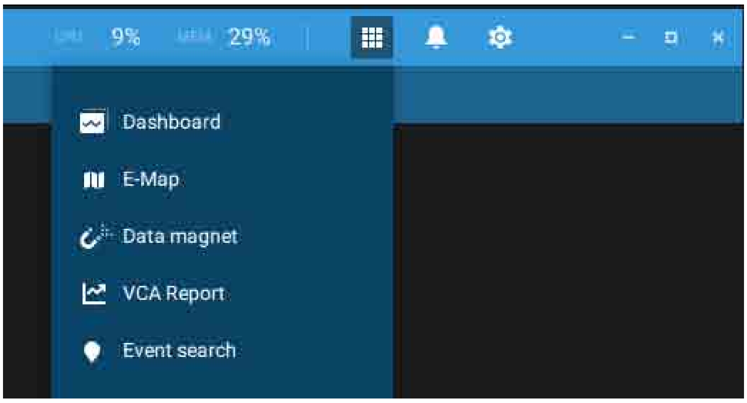
Google Map Settings

Google Map API Key

Map update frequency: 60 min

2-11. Event Search

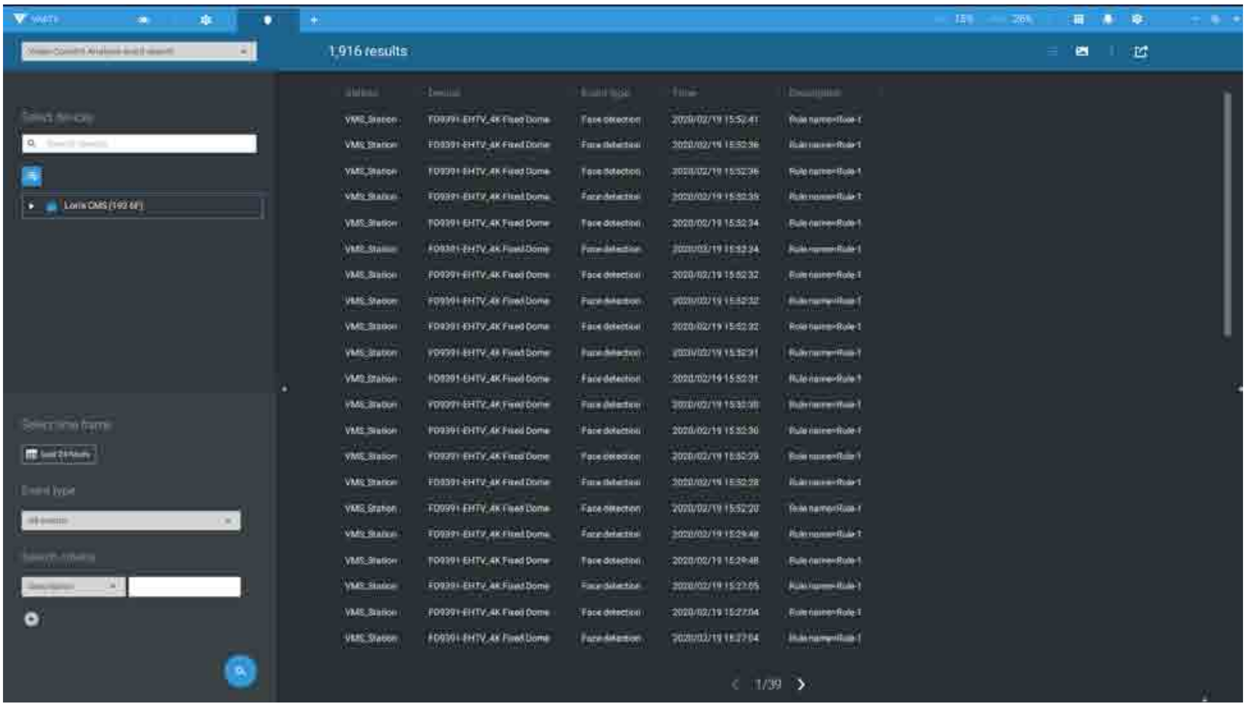
The Event Search window is accessed from the top tool bar.



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, Video Content Analysis events, and Trend Micro IoT Security events.

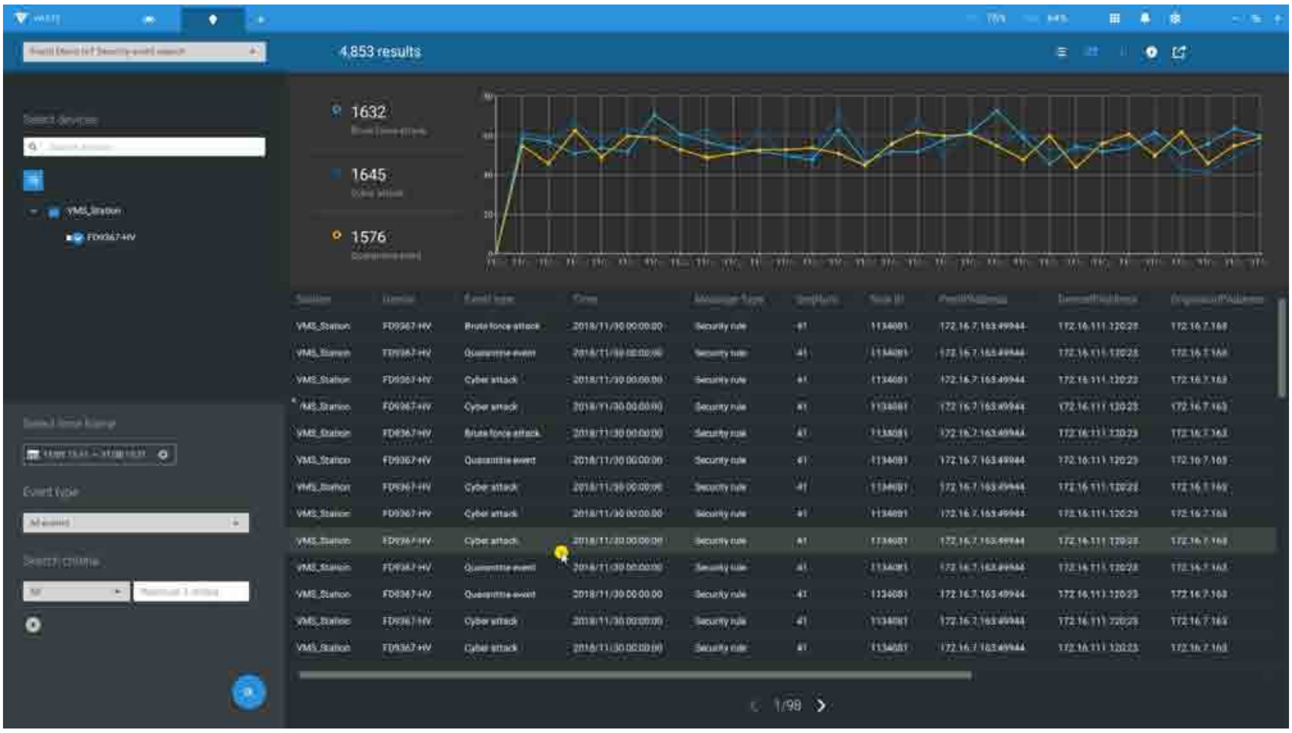
The sample screen for VCA-related events is shown below:



1,916 results

Station	Device	Event type	Time	Description
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:41	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:36	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:36	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:35	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:34	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:34	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:32	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:32	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:32	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:31	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:31	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:30	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:30	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:29	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:28	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:52:20	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:29:48	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:29:48	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:27:05	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:27:04	Rule name=Rule 1
VMS_Station	FD9391-EHTV_4K Fixed Dome	Face detection	2020/02/19 15:27:04	Rule name=Rule 1

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



4,853 results

1632 Brute force attack

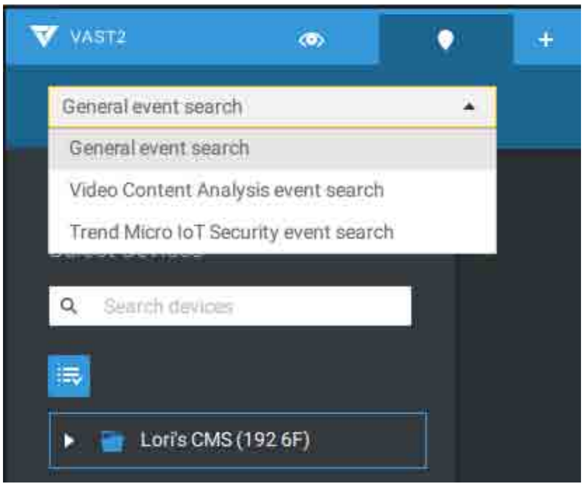
1645 Cyber attack

1576 Quarantine event

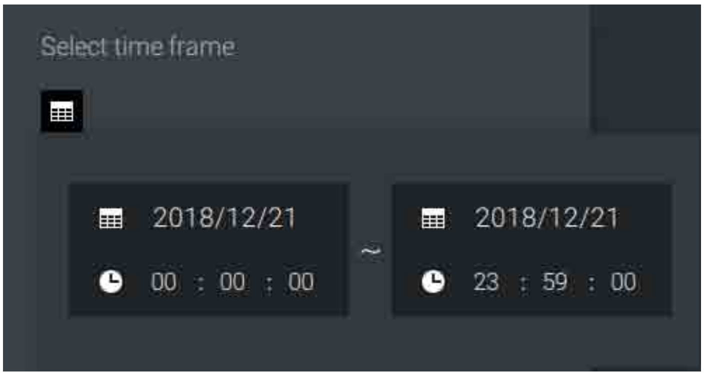
Station	Device	Event type	Time	Message Type	[illegible]	Rule ID	PeerIPAddress	DeviceIPAddress	OriginatorIPAddress
VMS_Station	FD9367-HV	Brute force attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Quarantine event	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Cyber attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Cyber attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Brute force attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Quarantine event	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Cyber attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Cyber attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Cyber attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Quarantine event	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Quarantine event	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Cyber attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163
VMS_Station	FD9367-HV	Cyber attack	2018/11/30 00:00:00	Security rule	41	1134081	172.16.7.163:49944	172.16.111.120:23	172.16.7.163

1/98

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).



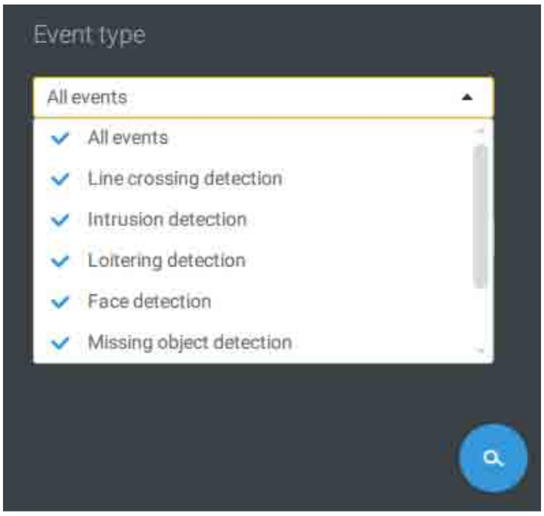
Use the calendar tool to specify the span of time as the search range.



Select time frame

2018/12/21 00 : 00 : 00 ~ 2018/12/21 23 : 59 : 00

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.

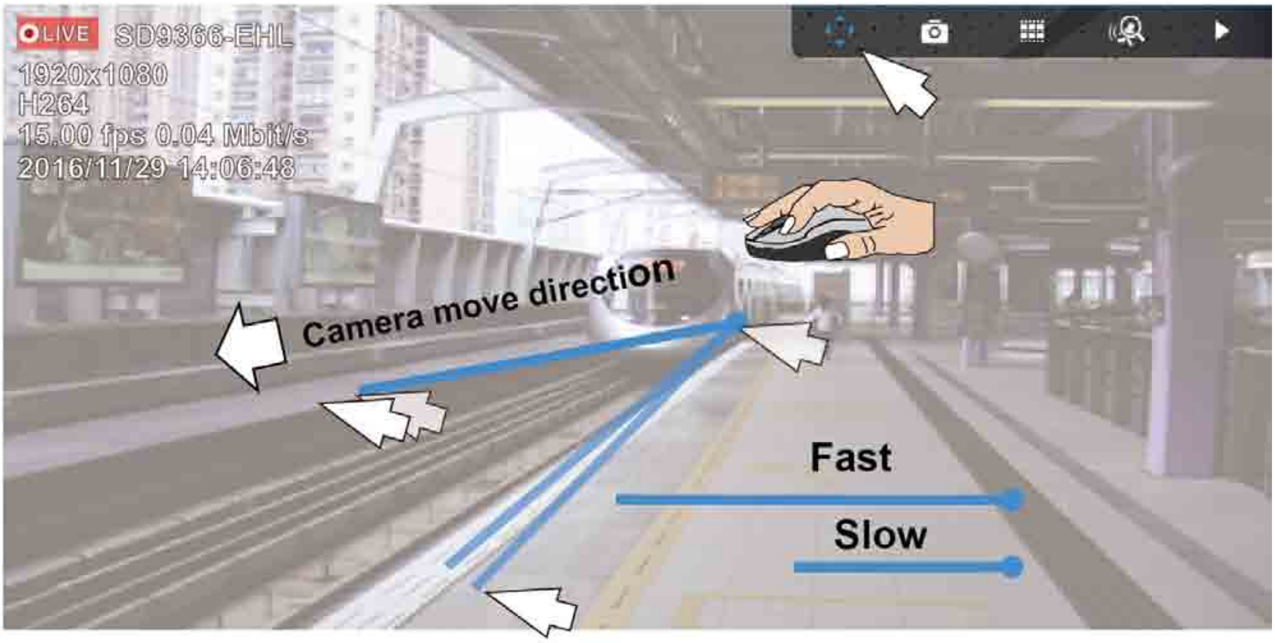


Click the search button to generate search results.

2-12. 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.

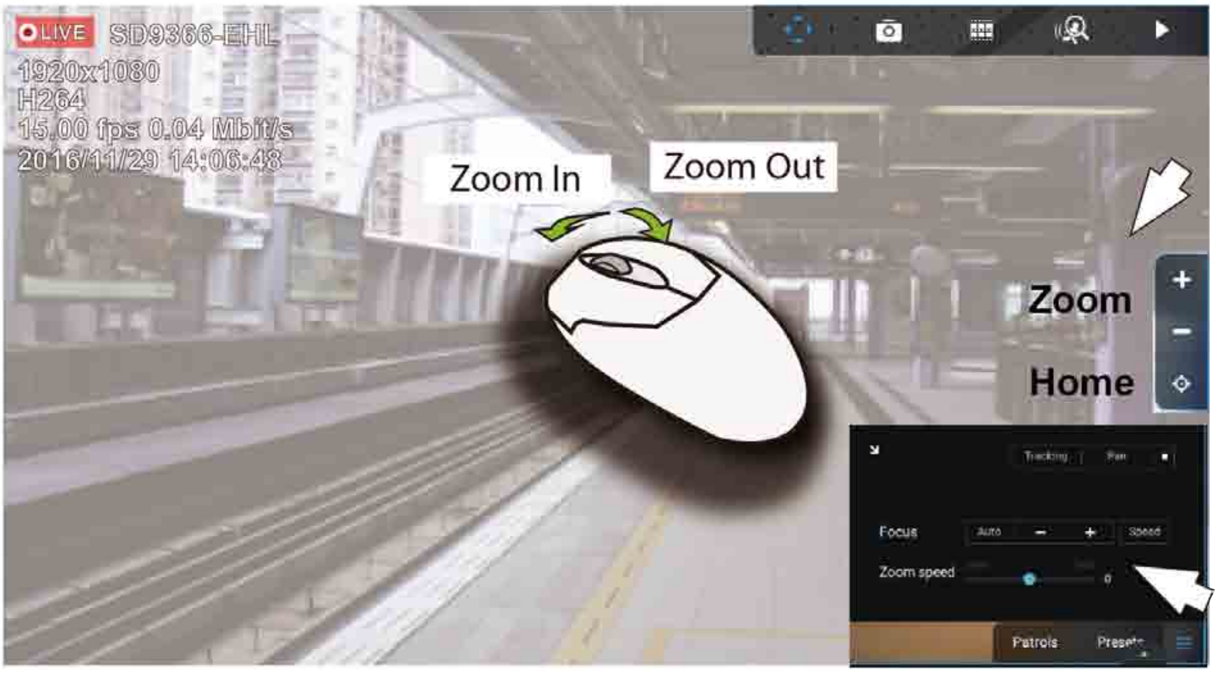
See Appendix D Joystick support if you use VIVOTEK's joystick.

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

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

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

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



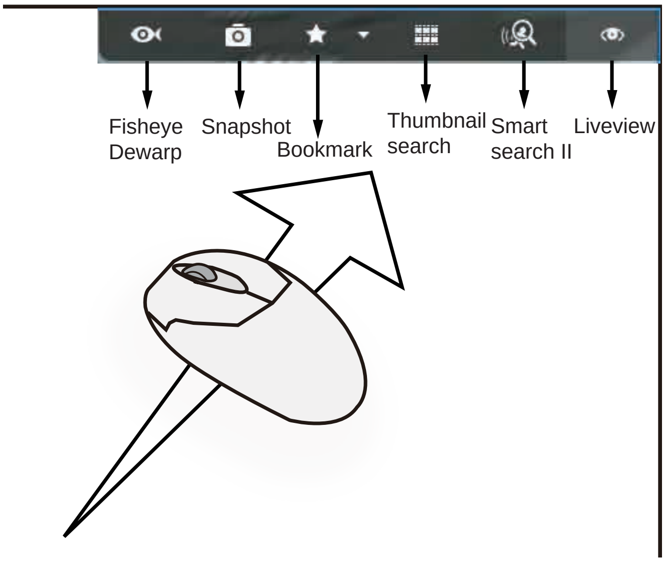
2-13. Playback

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:

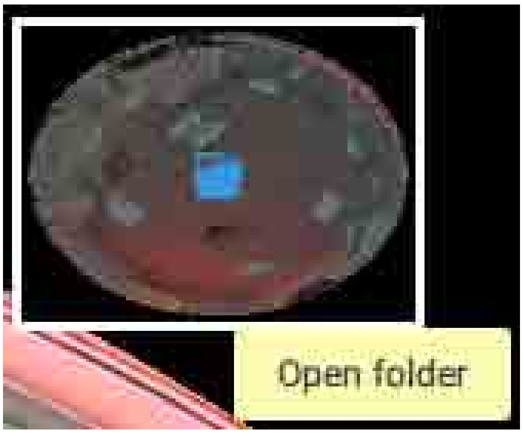
1. **Float Panel**: When Playback is started, swipe your mouse to the upper-right of the view cell to display the Playback float panel.



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.

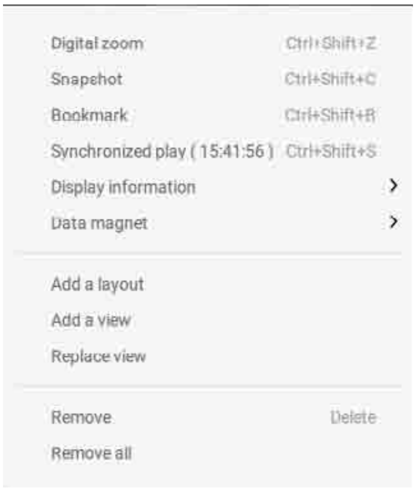


Bookmark: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos. Note that the bookmarked video clips are free from storage recycles. They will not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

Smart search II: Smart search II is an independent function. See page 117 for details.

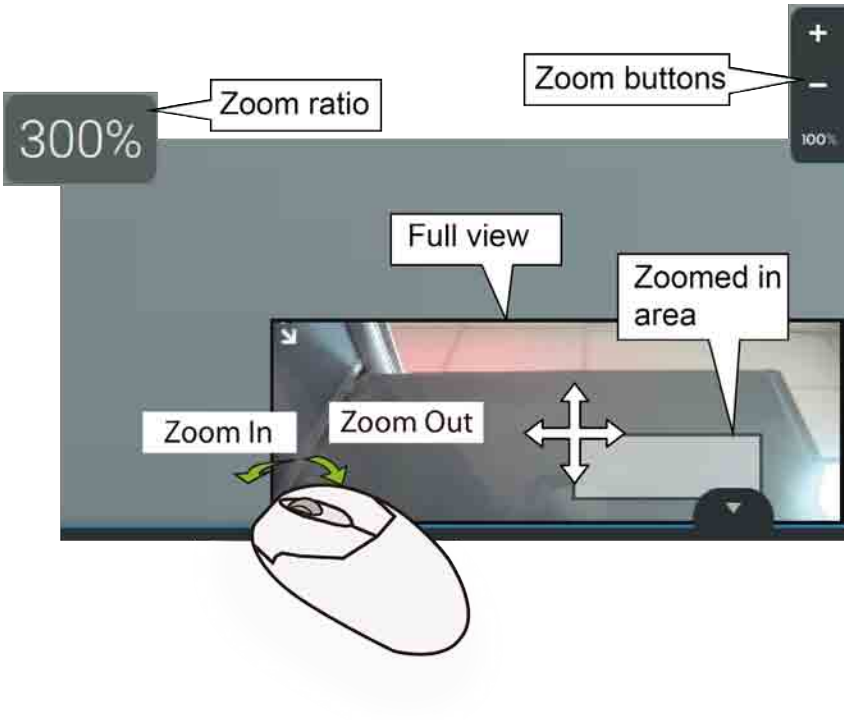
Liveview: Click to return to Live view.

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



Digital zoom	Ctrl+Shift+Z
Snapshot	Ctrl+Shift+C
Bookmark	Ctrl+Shift+B
Synchronized play (15:41:56)	Ctrl+Shift+S
Display information	›
Data magnet	›
Add a layout	
Add a view	
Replace view	
Remove	Delete
Remove all	

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



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

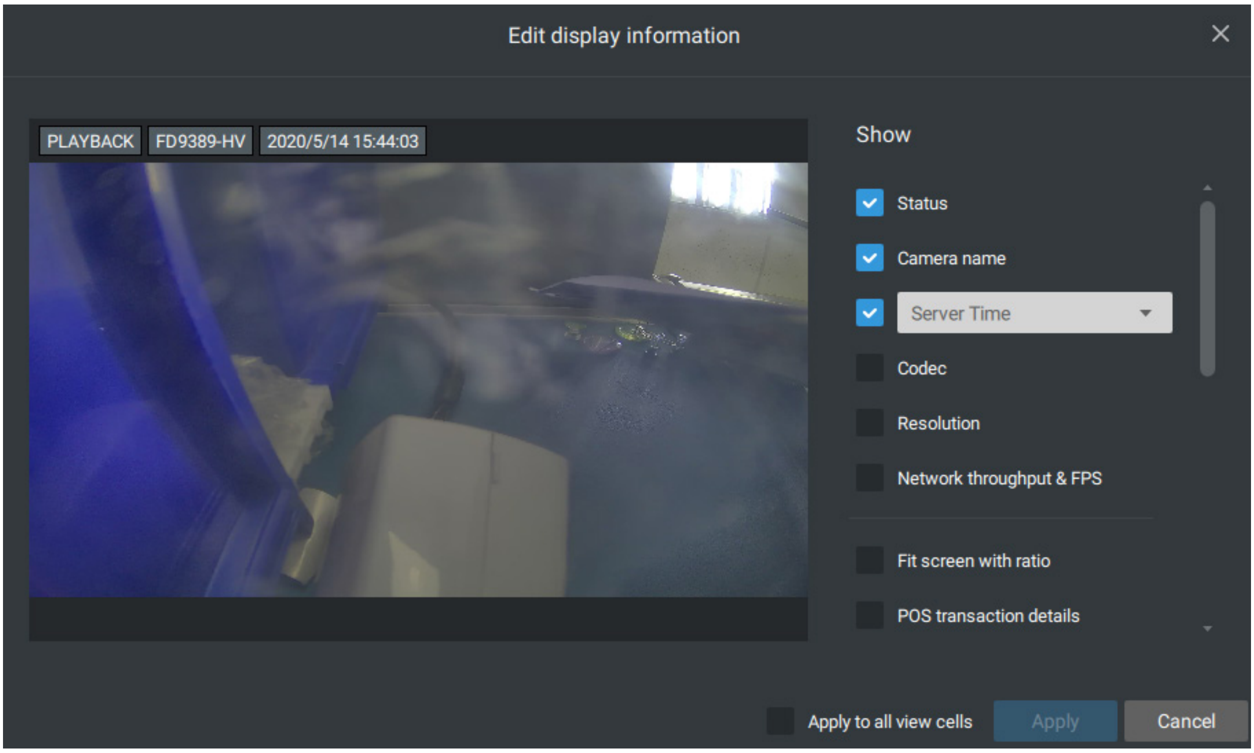
Bookmark: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos.

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

The following commands are general purpose commands.

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

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



Edit display information

Show

☑ Status

☑ Camera name

☑ Server Time

□ Codec

□ Resolution

□ Network throughput & FPS

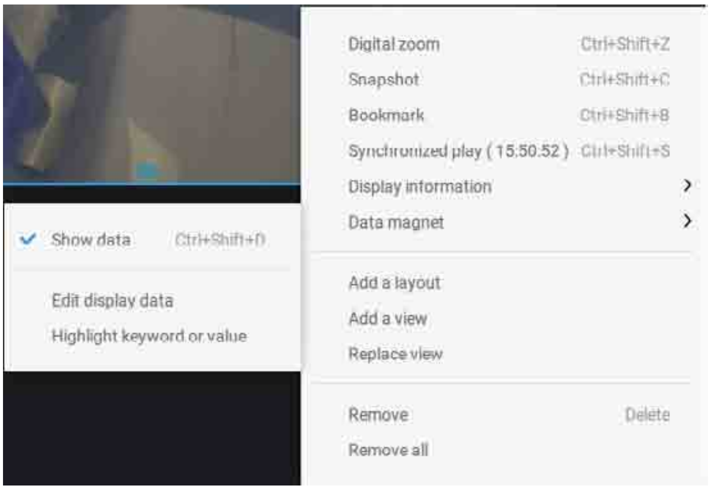
□ Fit screen with ratio

□ POS transaction details

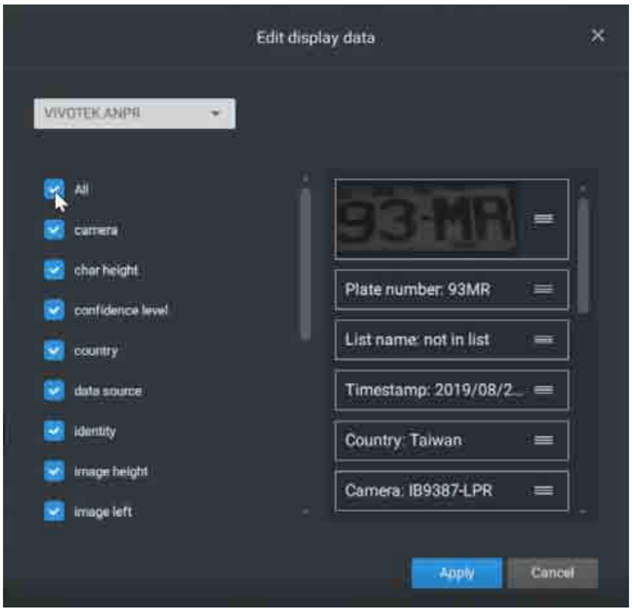
□ Apply to all view cells

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

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



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



VIVOTEK ANPR

☑ All
☑ camera
☑ char height
☑ confidence level
☑ country
☑ data source
☑ identity
☑ image height
☑ image left

93-MR

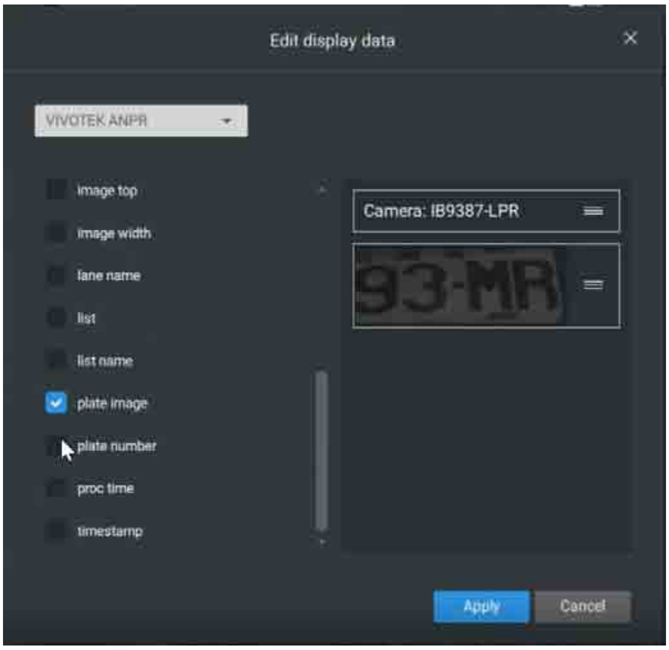
Plate number: 93MR

List name: not in list

Timestamp: 2019/08/2...

Country: Taiwan

Camera: IB9387-LPR



VIVOTEK ANPR

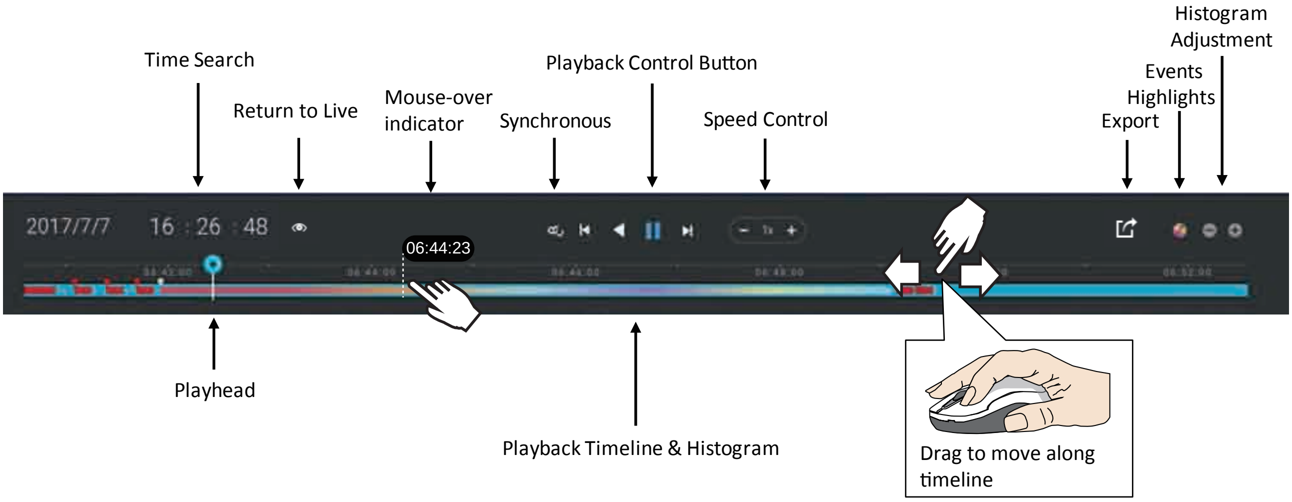
☐ image top
☐ image width
☐ lane name
☐ list
☐ list name
☑ plate image
☐ plate number
☐ proc time
☐ timestamp

Camera: IB9387-LPR

93-MR

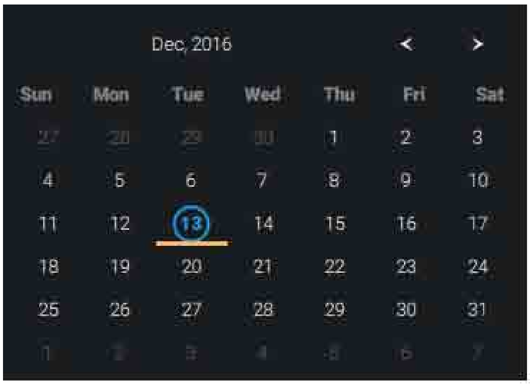
3. **Timeline Panel**: This panel appears when Playback is initiated.

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.



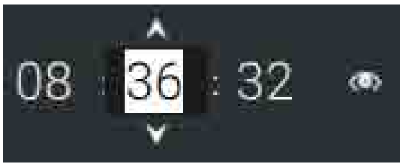
Starting from left to right, timeline control functions will be described as follolws:

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.

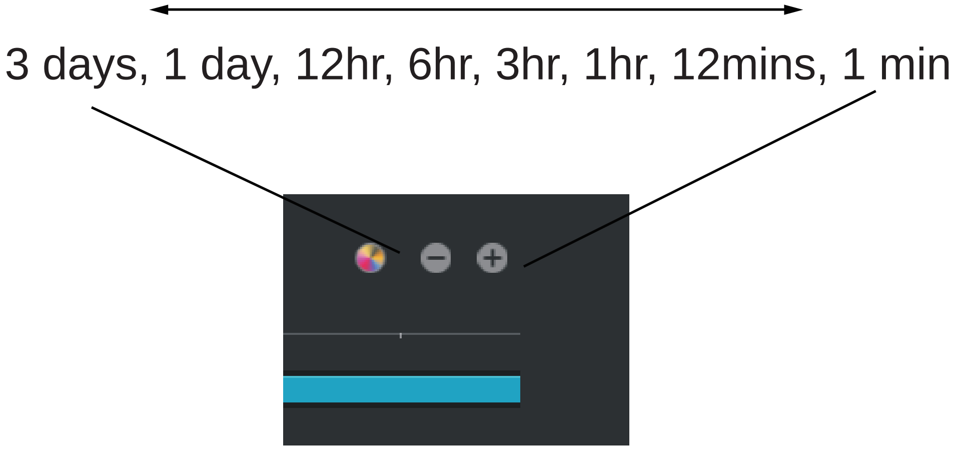


Blue: days with recordings.
Orange bottom line: Today.
White: days with no recordings.

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:

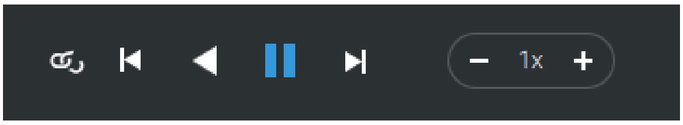

3 days, 1 day, 12hr, 6hr, 3hr, 1hr, 12mins, 1 min

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.

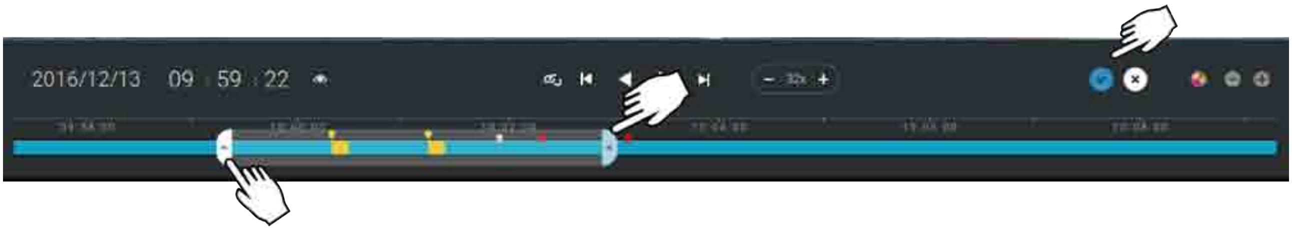
2-2. **Frame by frame buttons**: Click to move forward or backward to flick through the video frames. This may only display the I-frames.



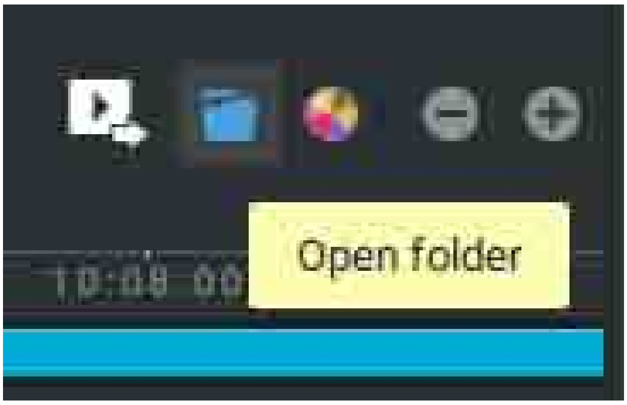
2-3. **Forward playback** and **reverse playback**: Click to view the video in the forward or reverse playback manner.

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

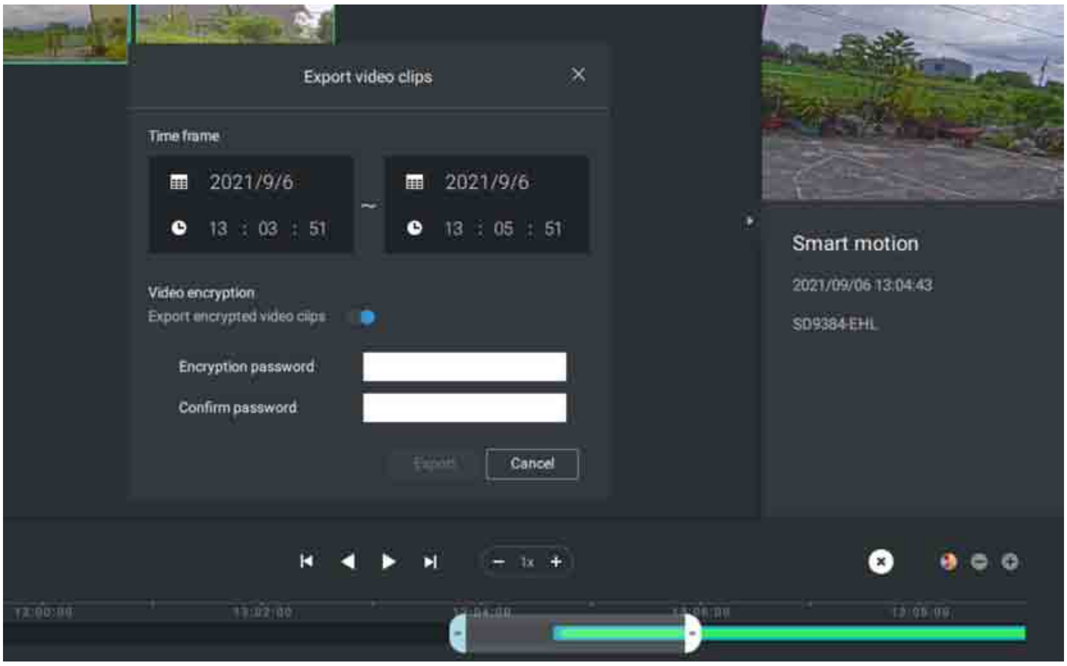
3. **Export Clips**: Click the Export Clips button . A range selector will appear. Pull the ends to include the time span you want to export. Note that each end of the selector, when clicked and selected, will turn white, and its location on the timescale is shown on the time line. When done, click the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



When you export a video, you can assign a password for the encrypted video. Once encrypted, you cannot play the video using ordinary video players. You can only play the video using VAST standalone player after you enter the correct password.



Export video clips

Time frame

2021/9/6 13 : 03 : 51 ~ 2021/9/6 13 : 05 : 51

Video encryption

Export encrypted video clips

Encryption password

Confirm password

Export Cancel

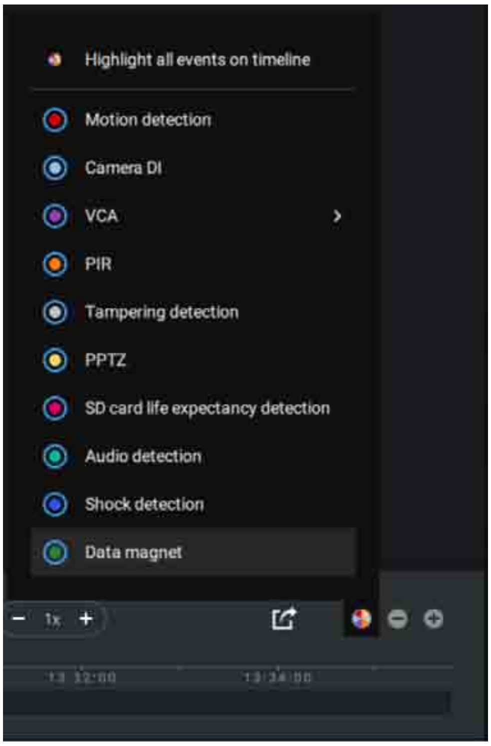
Smart motion

2021/09/06 13:04:43

SD9384-EHL

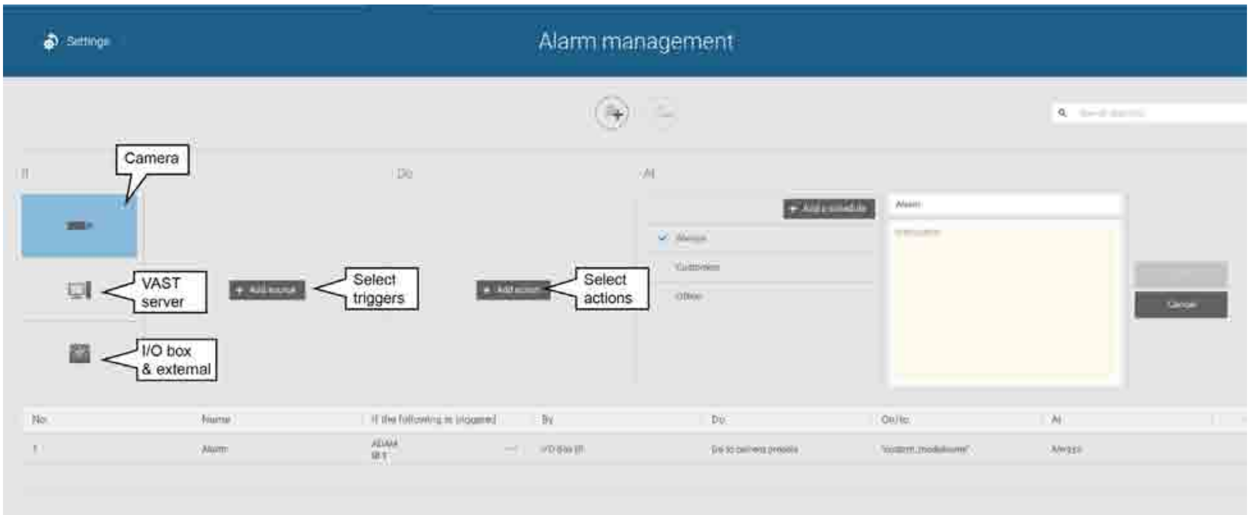
Event Highlights on timeline: Select one or all of the event types to display event tags on the timeline that match those have occurred in the past.

Note that on the VIVOTEK's Linux-based NVR, the timeline will display the occurrence of an event for a length of 10 seconds since its occurrence.



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.

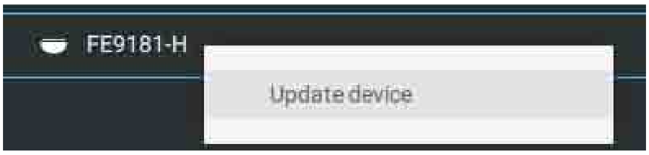


A wide variety of triggering conditions can be applied, including:

1. Camera triggers ▬▪

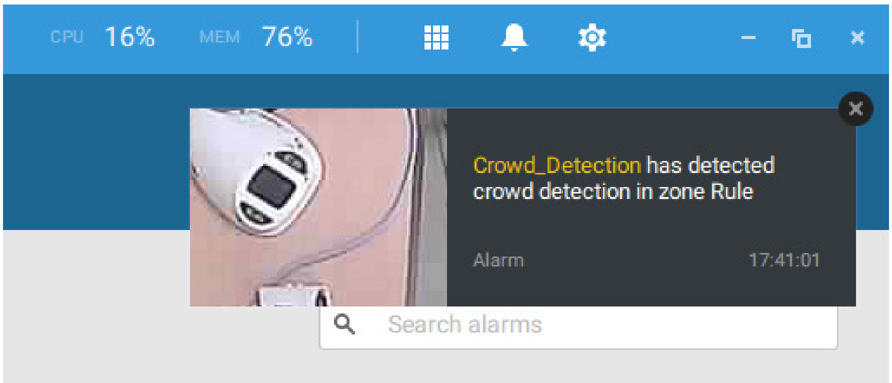
General			
●	Motion detection	●	IR (Infrared)
●	Camera DI	●	PIR (Passive Infrared)
●	Camera DO	●	Tampering detection
●	Temperature	●	Stop recording
●	Recording error	●	Audio detection
●	Video loss (Video server only)	●	Shock detection
●	SD card life expectancy detection		
Video Content Analysis			
●	Line crossing (VCA)	●	Intrusion detection
●	Loitering detection	●	Face detection
●	Missing object detection	●	Unattended object detection
●	Crowd detection	●	Smart tracking
●	Zone detection	●	People running detection
●	Parking Violation detection	●	Restricted Zone 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.

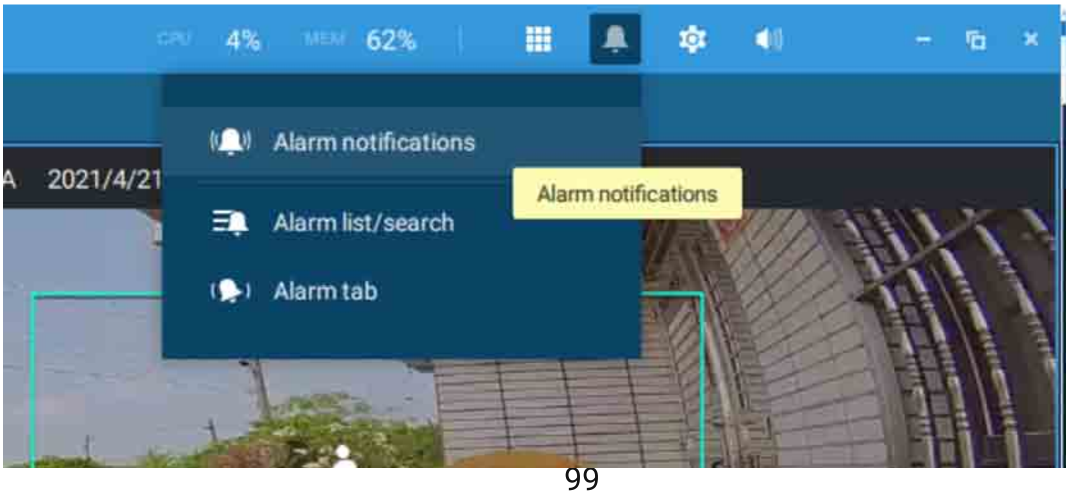
If a triggering condition is associated with event recording, an event prompt will pop up on the screen when a triggering condition is met. For example, the number of people exceeds a preset threshold in a Crowd Detection configuration. The sample prompt is shown below. The related footage can be played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



Crowd_Detection has detected crowd detection in zone Rule

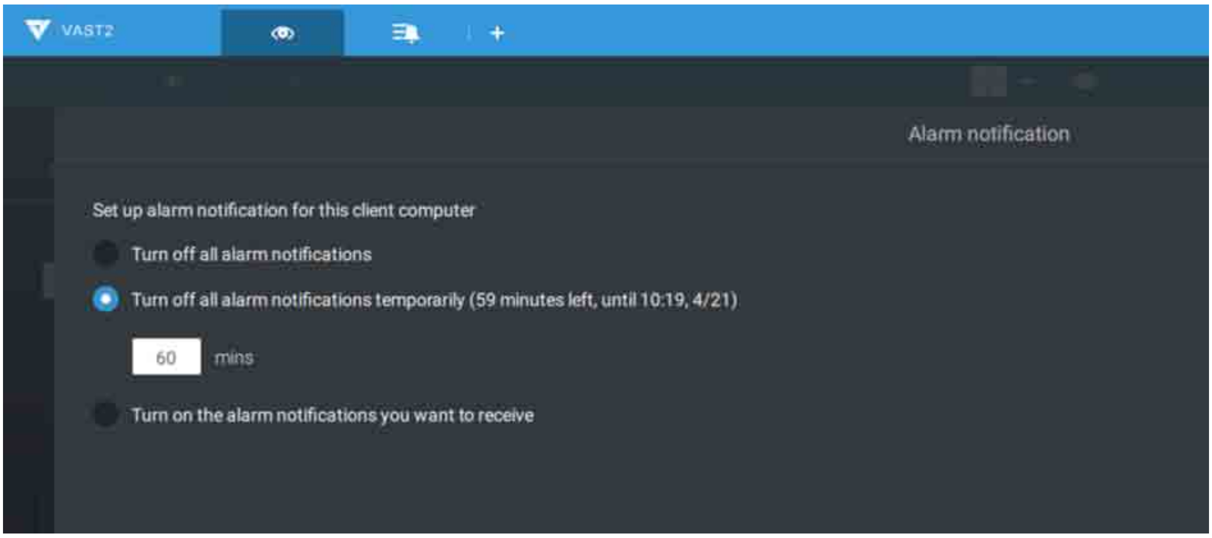
The alarm notification can be turned off by clicking on the Alarm tab. You can enter the time span when you do not want to receive notifications and the notifications will automatically turn on after the time span. Enter the number in the mins field. The max. time span is 9,999 minutes.

The notification configuration is kept on the client computer.
When the Alarm notification is turned off, the Alarm tab icon is greyed out 🔔.



Individual VAST clients can configure which kinds of alarms can be delivered to them by selecting the alarm types listed in "Turn on the notifications you want to receive." When the individual alarms are turned off, the following client-side alarm actions will be disabled on the client computers:

1. Notification.
2. Send live streaming.
3. Go to E-map.
4. Sound the alarm.



Alarm notification

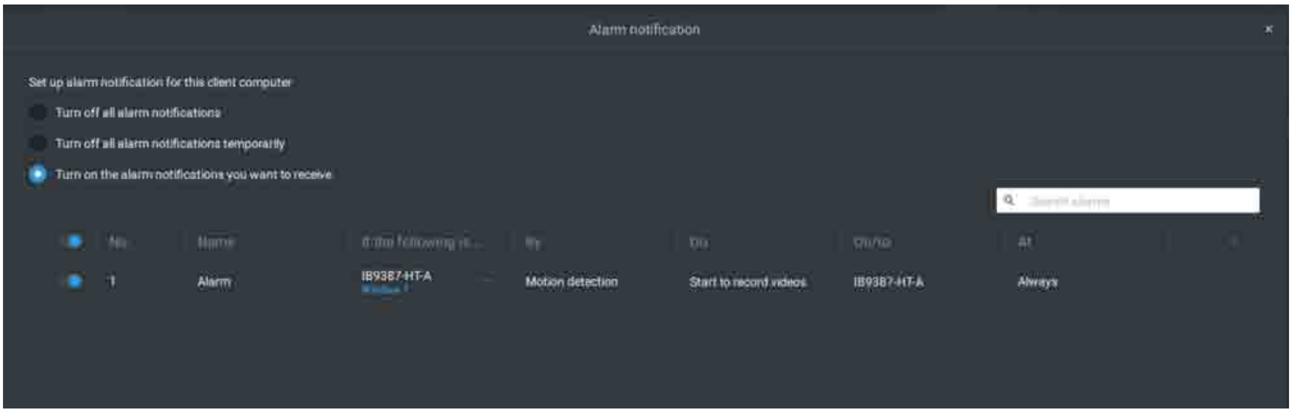
Set up alarm notification for this client computer

○ Turn off all alarm notifications

● Turn off all alarm notifications temporarily (59 minutes left, until 10:19, 4/21)

60 mins

○ Turn on the alarm notifications you want to receive



Alarm notification

Set up alarm notification for this client computer

○ Turn off all alarm notifications

○ Turn off all alarm notifications temporarily

● Turn on the alarm notifications you want to receive

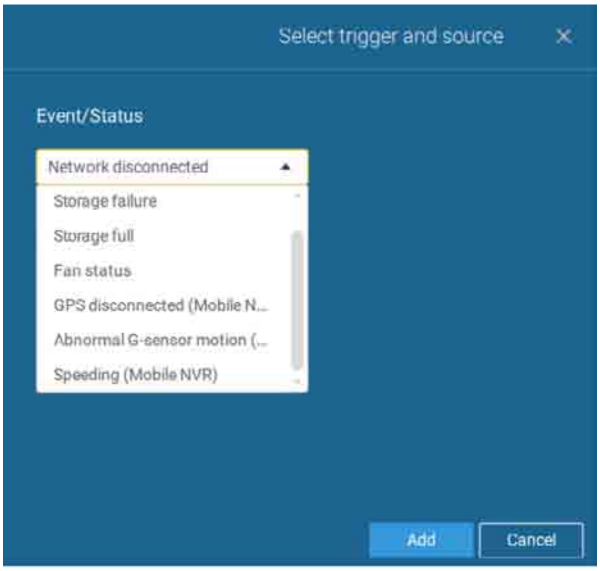
●	No.	Name	If the following is...	By	Do	On/to	At
●	1	Alarm	IB9387-HT-A Window 1	Motion detection	Start to record videos	IB9387-HT-A	Always

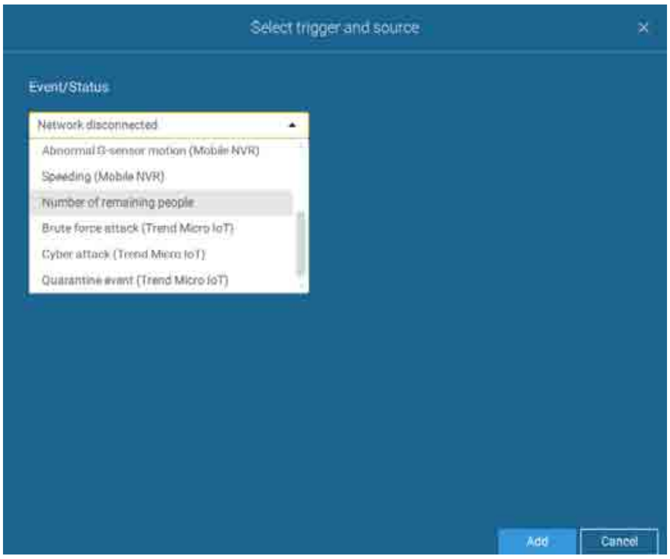
Note that the default for the alarm notification is "Turn on the alarm notification you want to receive." If you turn off the alarm notification, you need to re-activate it after you turn off the notification the first time.

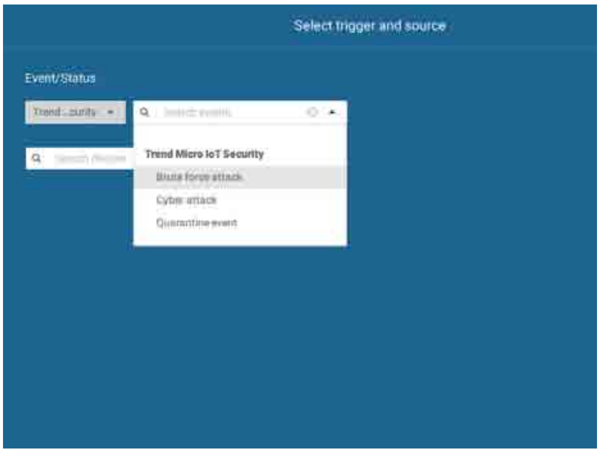
2. VAST server and NVR triggers

●	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 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.




Select trigger and source
Event/Status
Network disconnected
Abnormal G-sensor motion (Mobile NVR)
Speeding (Mobile NVR)
Number of remaining people
Brute force attack (Trend Micro IoT)
Cyber attack (Trend Micro IoT)
Quarantine event (Trend Micro IoT)
Add
Cancel



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."

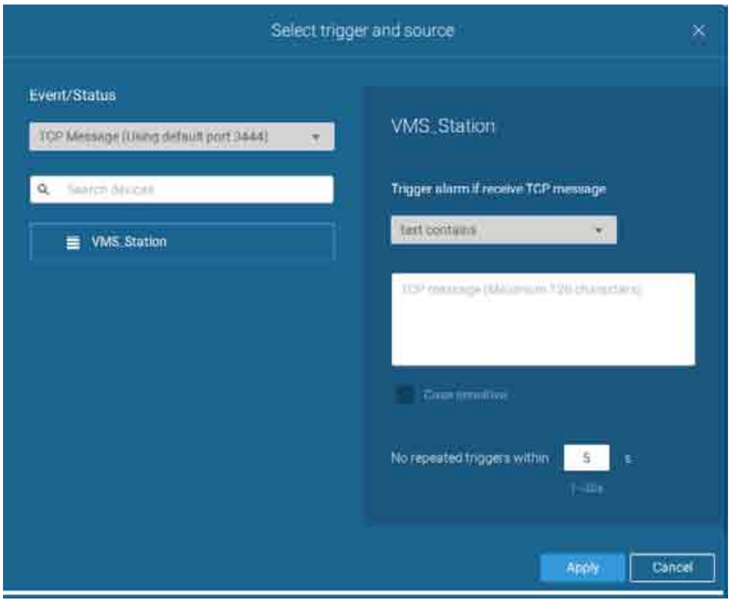
For I/O box configuration, please refer to the I/O Box page.

3. I/O box and TCP triggers

●	DI/DO Device DI	This applies when an external I/O box is applied, e.g., Advantech's ADAM I/O box.
●	DI/DO Device DO	
●	TCP Message	TCP message comes from the peer VAST servers or external sources (such as an access control system) via the analysis of received TCP message over the 3444 port. This is a paid feature.
●	Data Magnet	Triggering conditions can be acquiring data from 3rd-party software, such as the character height, image width, list, list name, country, from an LPR software, etc.
●	Virtual trigger	A virtual trigger allows users to create a button on live view to trigger Alarm actions, e.g., go to a camera preset, add bookmark, play an audio file, send HTTP requests, etc.

To configure a TCP message trigger,

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


Select trigger and source

Event/Status

TCP Message (Using default port 3444)

Search devices

VMS_Station

VMS_Station

Trigger alarm if receive TCP message

text contains

TCP message (Maximum 128 characters)

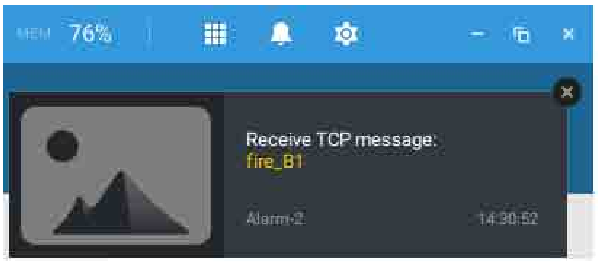
Case sensitive

No repeated triggers within 5 s

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.


MEM 76%

Receive TCP message:
fire_B1

Alarm-2 14:30:52

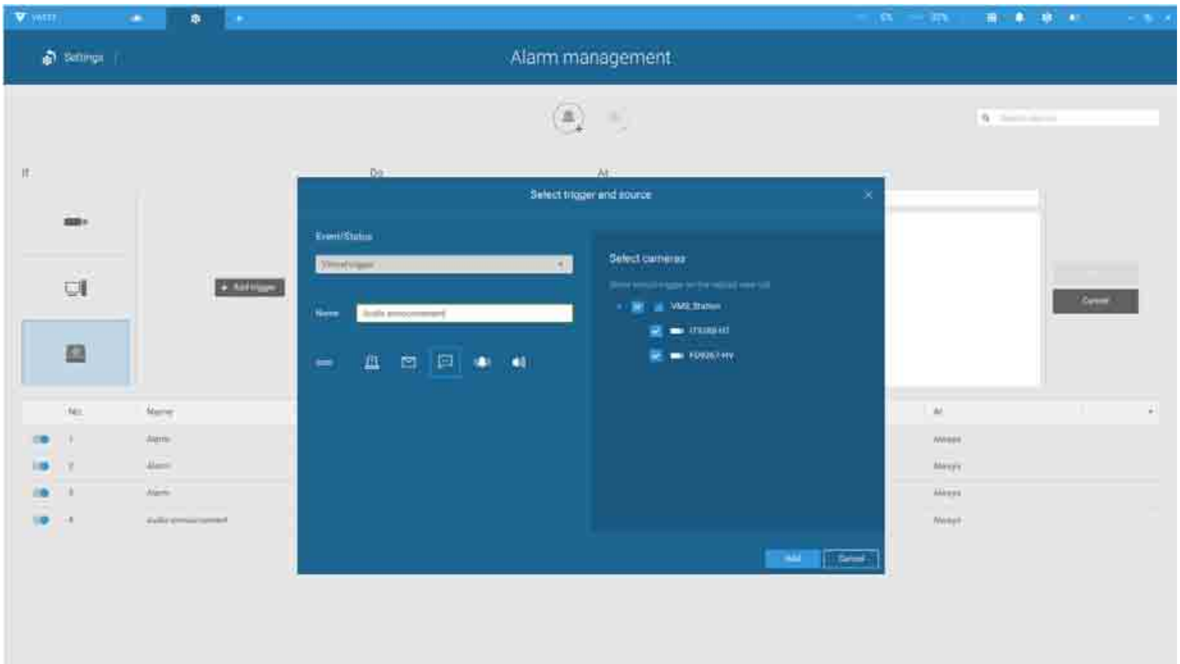
Virtual triggers have the following benefits:
1. More operation control, e.g., got to camera preset, add bookmark, play audio file with netwok audio devices.
2. Integrating 3rd-party systems and devices, using the Send HTTP requests, Set DO status commands.

To configure a Virtual trigger,

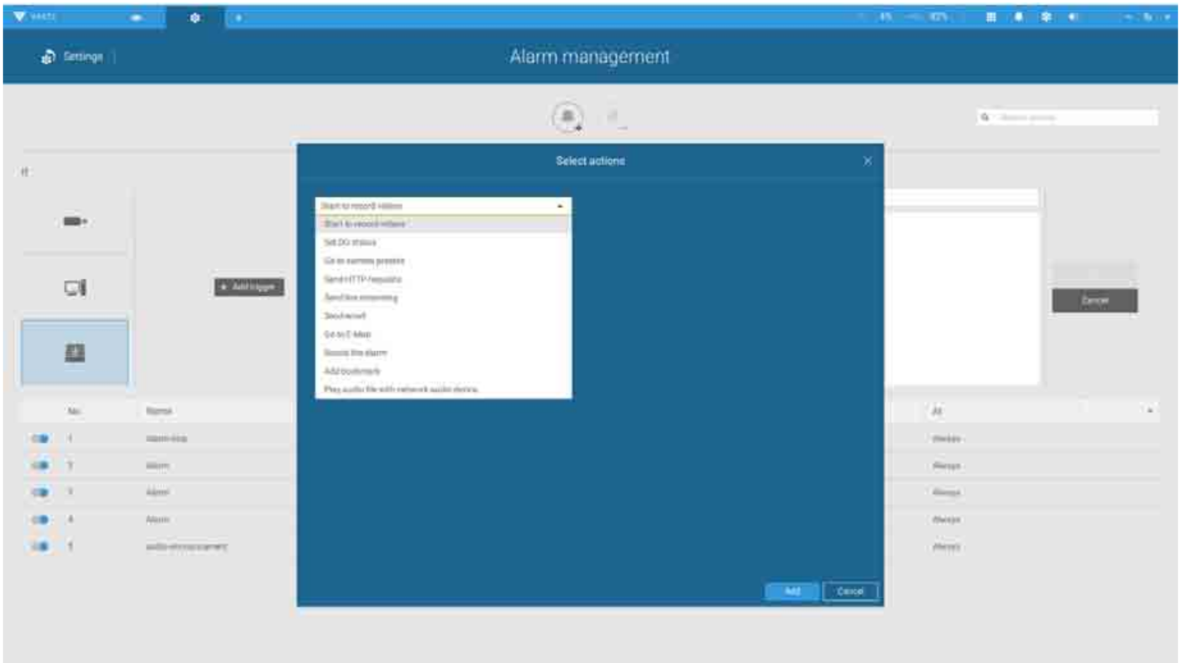
Go to Settings > Alarm > Add alarm.

Select the External device event, and then click on the Add trigger button.

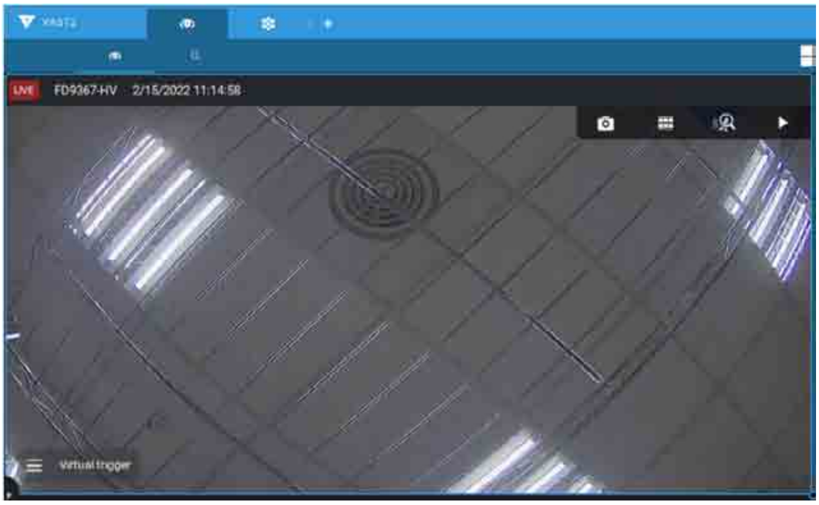
The Select trigger and source window will prompt.



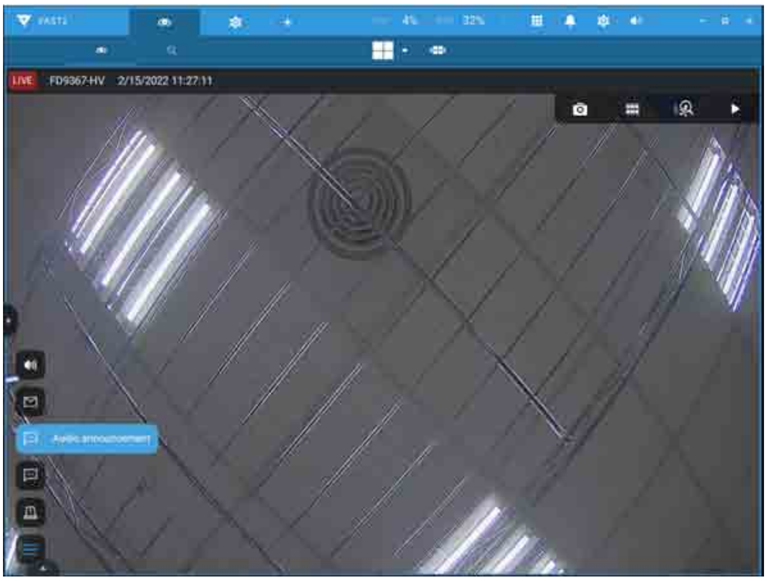
Select the alarm action.



With a pre-configured virtual trigger, a trigger button appears on the live view.



When activated, all of virtual trigger buttons will appear allowing you to perform the associated actions.



The available actions include:

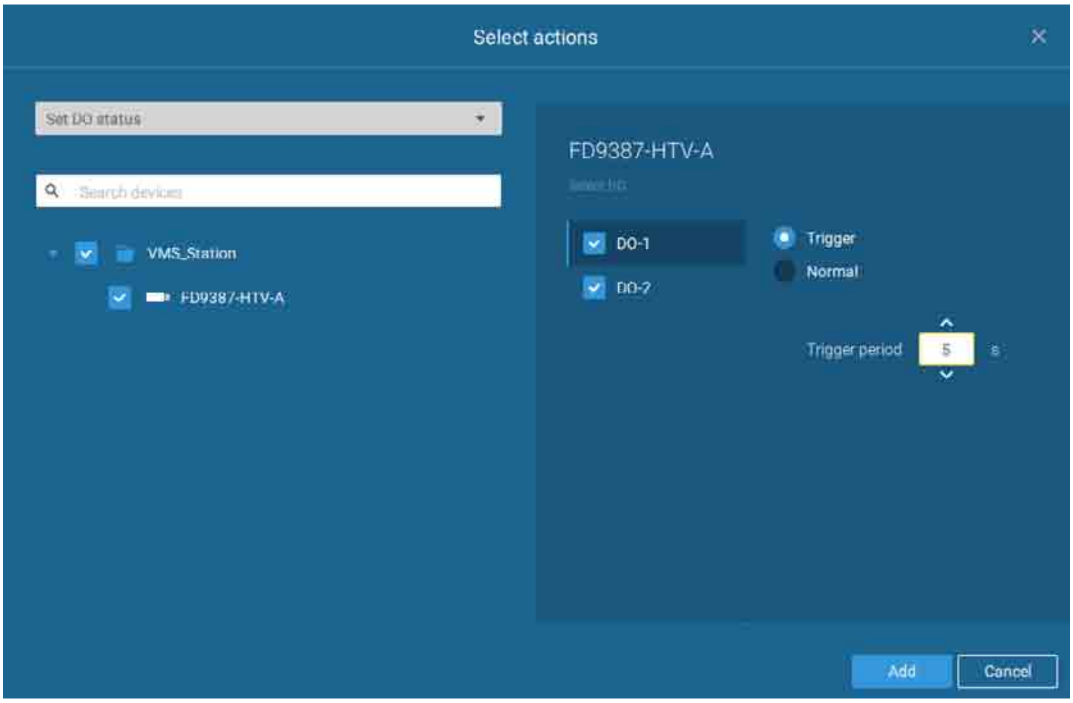
●	Start to record video	●	Send HTTP requests
●	Set DO status	●	Send live streaming
●	Go to camera presets	●	Send email
●	Go to E-map	●	Sound the alarm
●	Add bookmark	●	Play audio file with network audio device

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

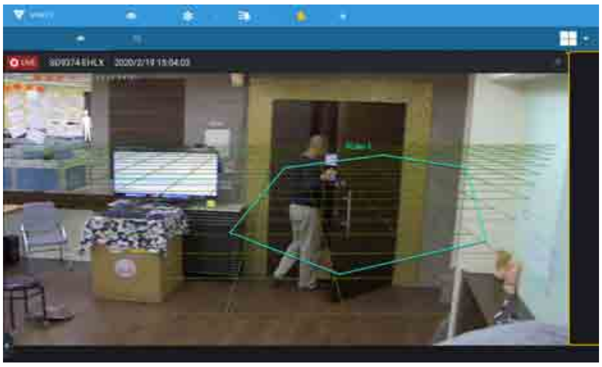
The Set DO status will activate a DO connection. For example, to light an illuminator or sound an alarm.

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

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



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



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

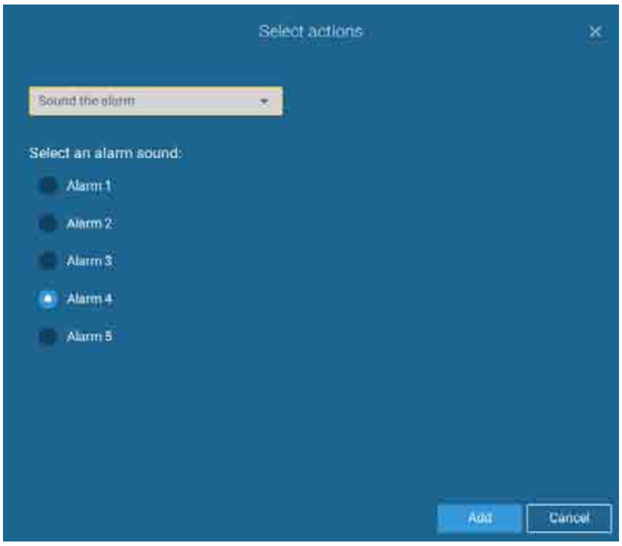
The VAST server automatically disables unavailable options. For example, when the DO option is selected, the cameras that do not support DO connections will be hidden.

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

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

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

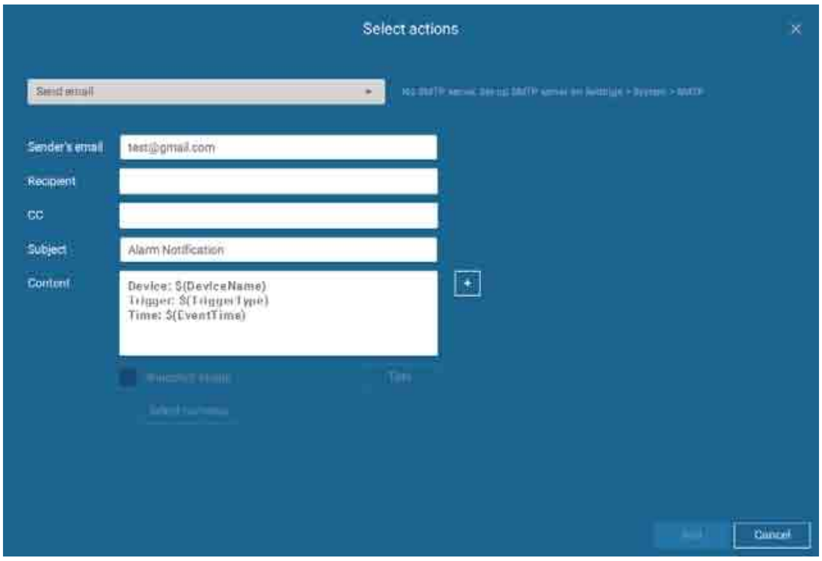
The Sound the alarm action provides 5 alarm sounds that will be sounded on the VAST client or server. Your VAST client or server should have speakers for playing the audible alarm.



Select an alarm sound:

- ○ Alarm 1
- ○ Alarm 2
- ○ Alarm 3
- ● Alarm 4
- ○ Alarm 5

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



No SMTP server. Set up SMTP server on Settings > System > SMTP

Sender's email: test@gmail.com

Recipient:

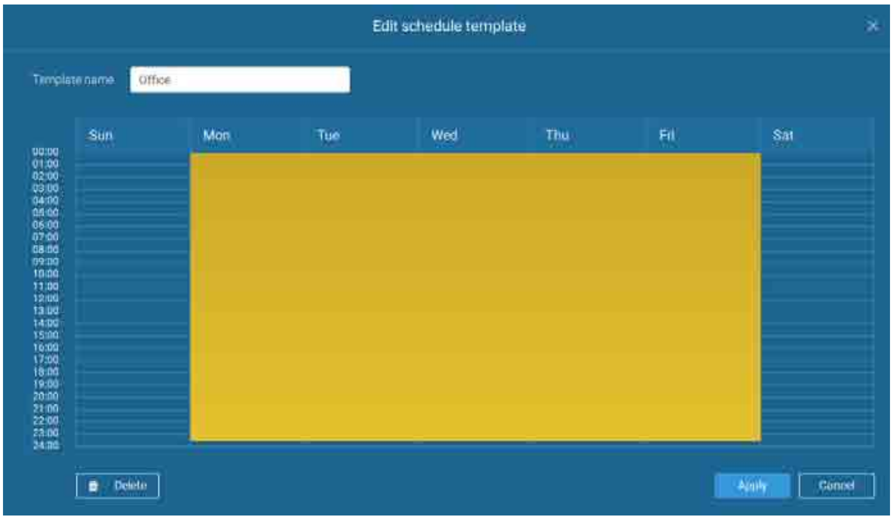
CC:

Subject: Alarm Notification

Content:

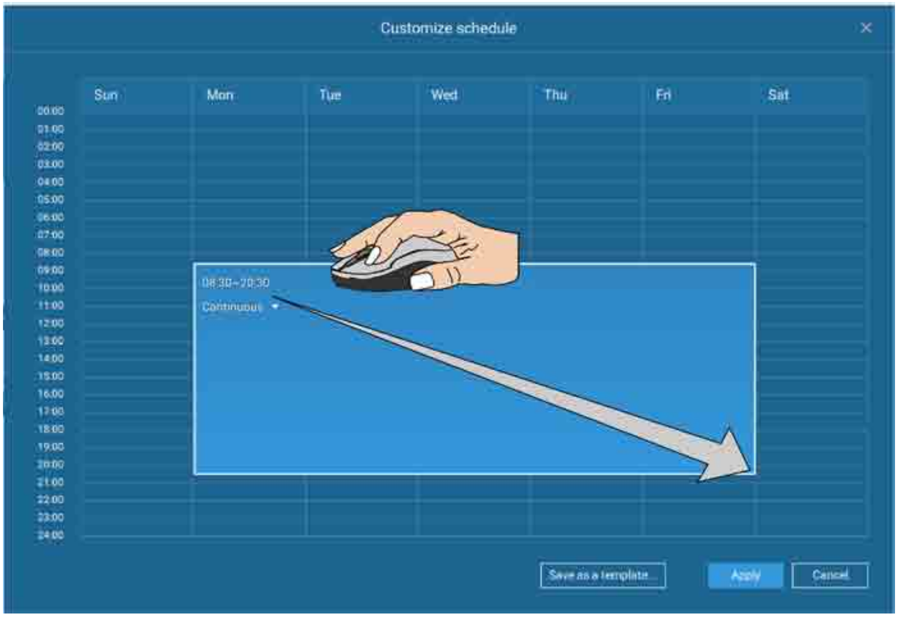
```
Device: $(DeviceName)
Trigger: $(TriggerType)
Time: $(EventTime)
```

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.


Template name: Office

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

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


08:30~20:30
Continuous

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.

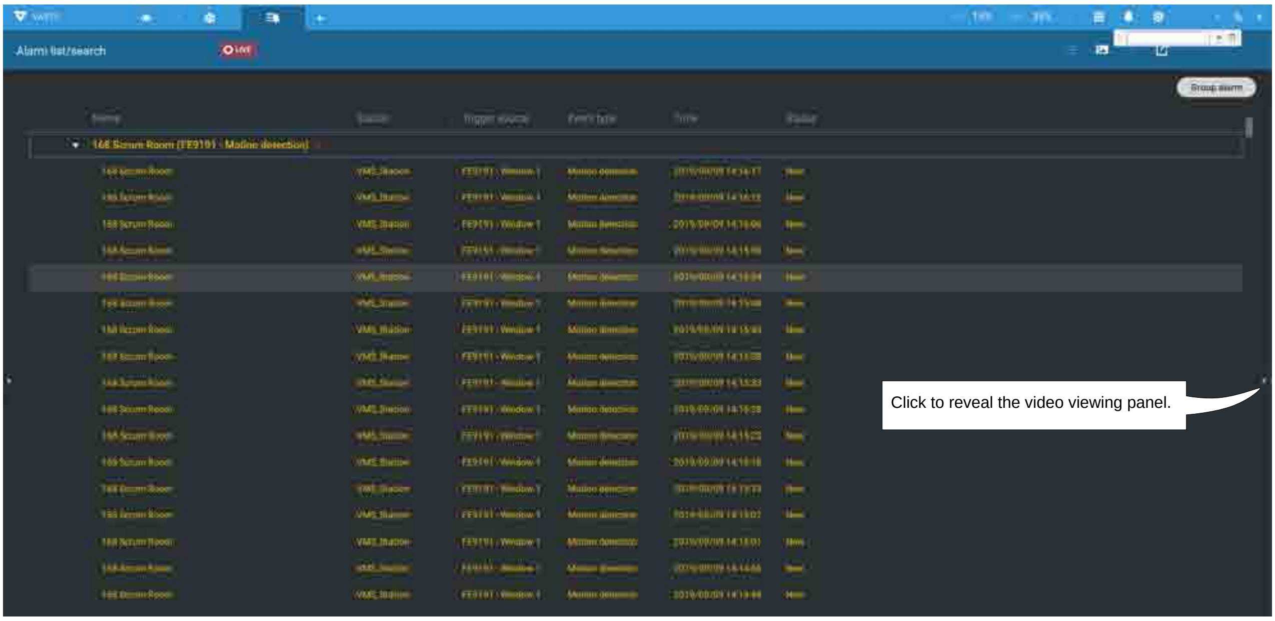
Enter a name and instructions for users to follow, and then click Add to complete the Alarm setting.

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.

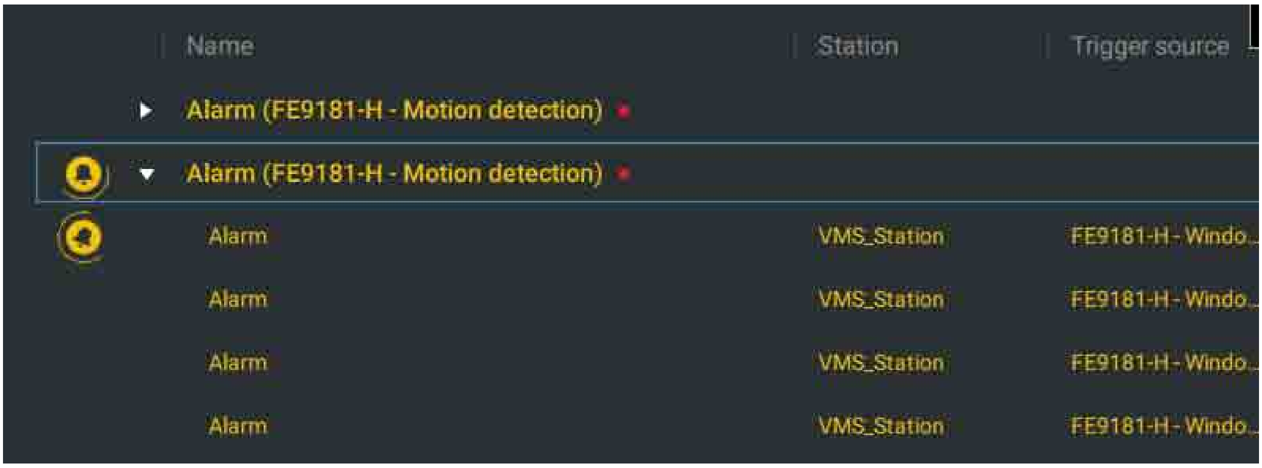
On the alarm list, click the Group alarm button to display the alarm group.



Click to reveal the video viewing panel.

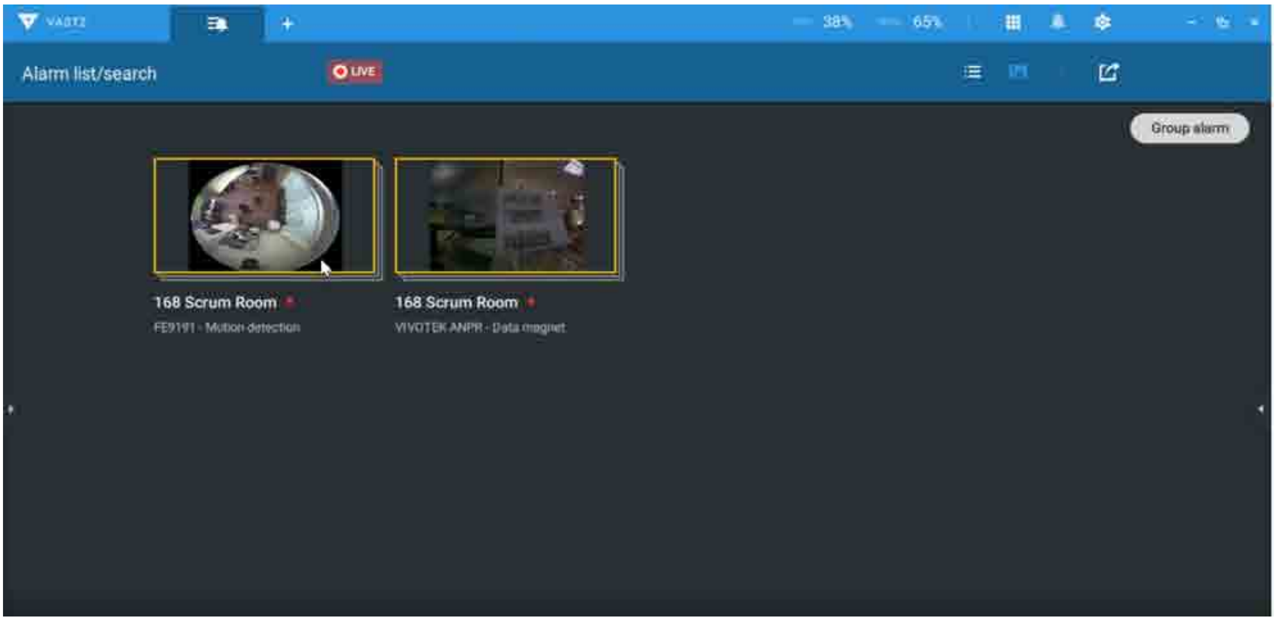
In the list mode, you can expand the right-hand-side panel. The video of the latest alarm will display.

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

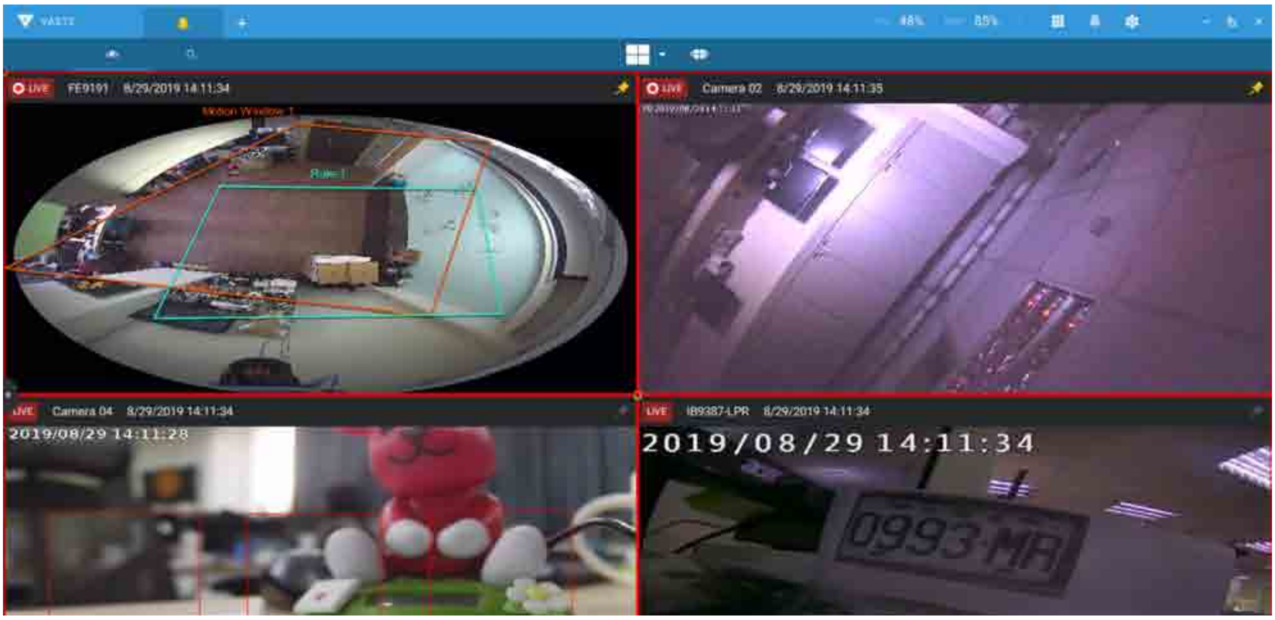


Name	Station	Trigger source
▸ Alarm (FE9181-H - Motion detection) ●		
▾ Alarm (FE9181-H - Motion detection) ●		
Alarm	VMS_Station	FE9181-H - Windo...
Alarm	VMS_Station	FE9181-H - Windo...
Alarm	VMS_Station	FE9181-H - Windo...
Alarm	VMS_Station	FE9181-H - Windo...

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



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



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

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

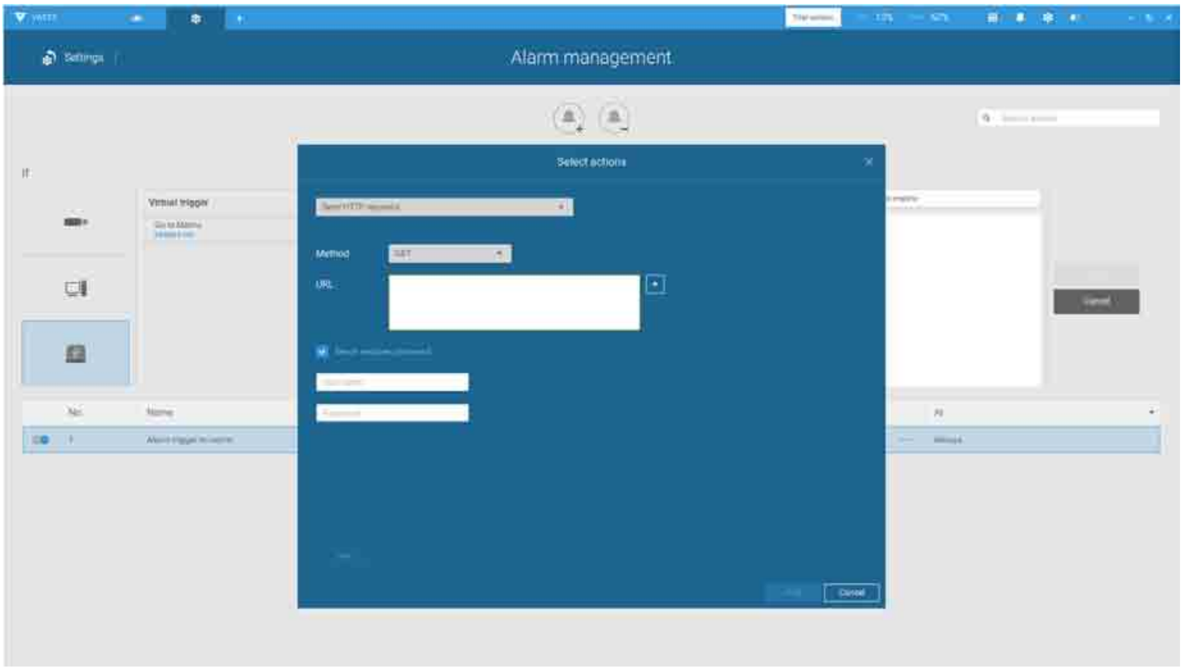
Configuring Send HTTP requests

When configured, the server will send an HTTP request protocol to a 3rd-party device or application. The HTTP request supports GET and POST commands.

The GET method is to request data from a specified resource.

The POST method is used to send data to a server to create or update a resource.

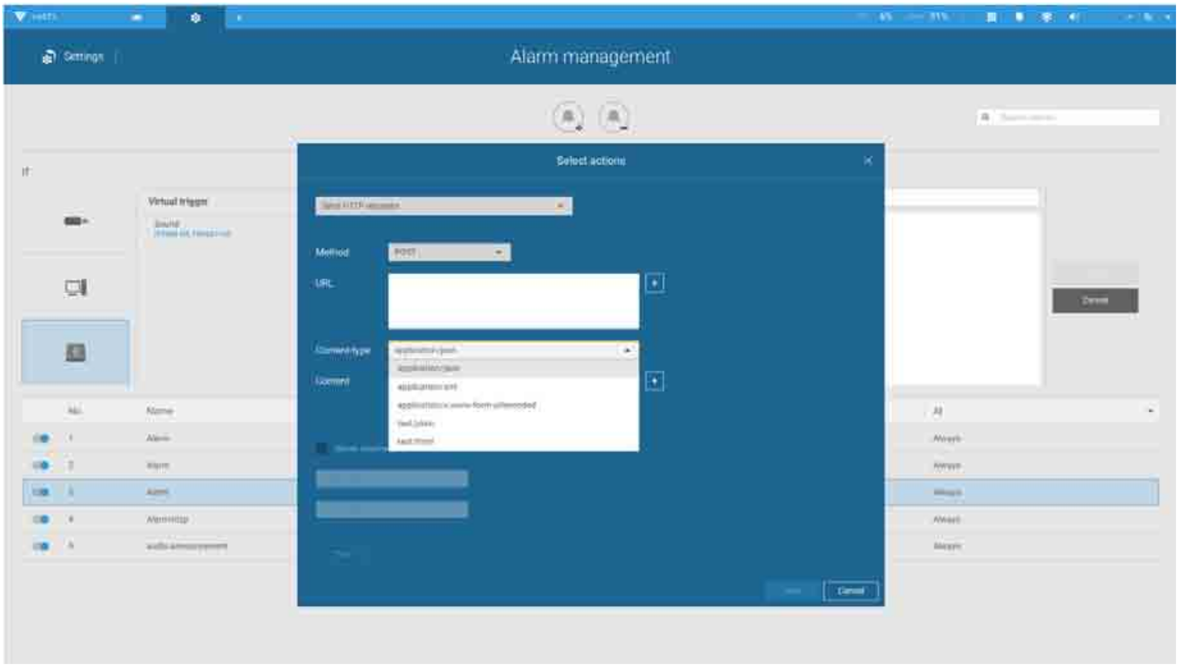
Below is a screen for setting the GET command. Enter the target resource's URL address.



Method: GET

URL:

Below is a screen for setting the POST command. Enter the target resource's URL address, the content, and select the content type. If the need should arise for more content types, you can contact VIVOTEK's technical support.



Method: POST

URL:

Content type: application/json

- application/json
- application/xml
- application/x-www-form-urlencoded
- text/plain
- text/html

Content:

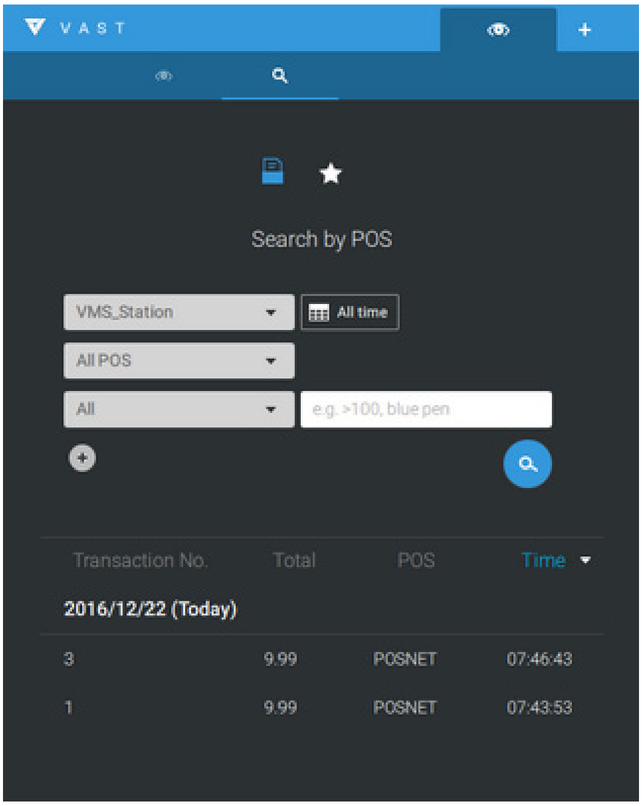
2-15. Search Panel

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.

2. 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 the 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.



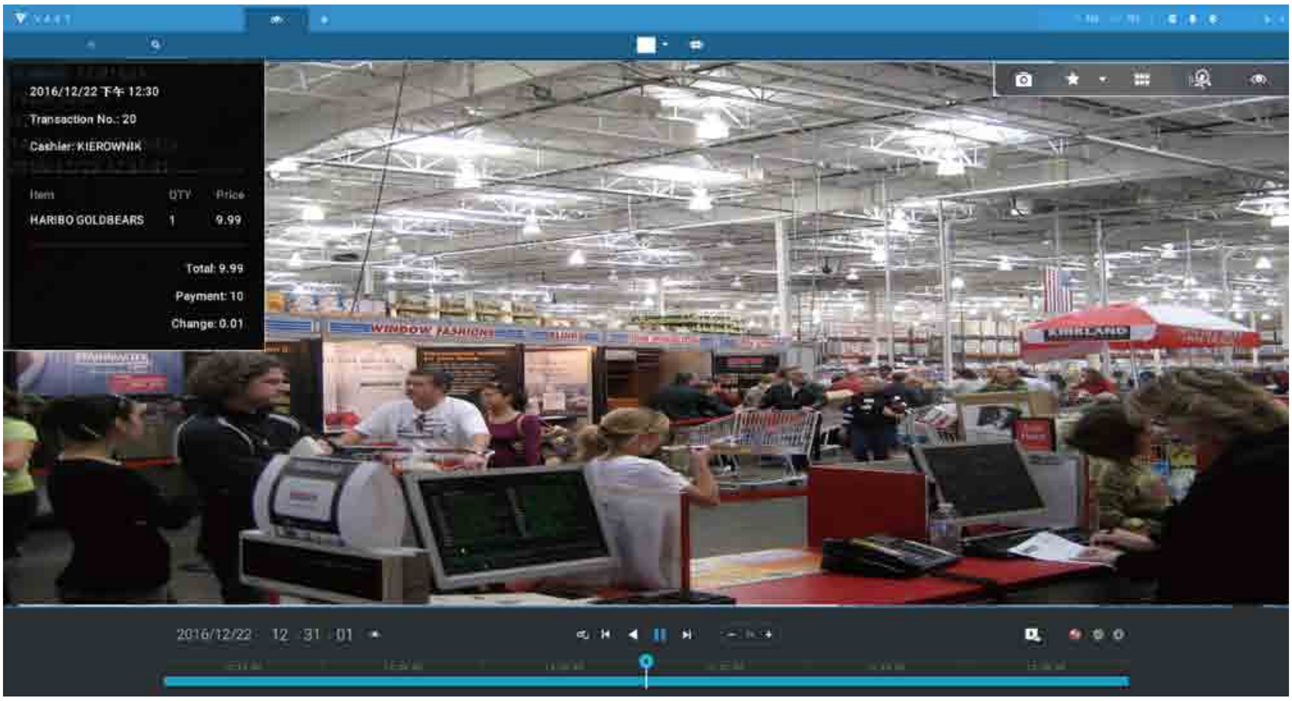
Search by POS

VMS_Station ▾ | All time
All POS ▾
All ▾ | e.g. >100, blue pen

Transaction No.	Total	POS	Time ▾
2016/12/22 (Today)			
3	9.99	POSNET	07:46:43
1	9.99	POSNET	07:43:53

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.



2016/12/22 下午 12:30

Transaction No.: 20

Cashier: KIEROWNIK

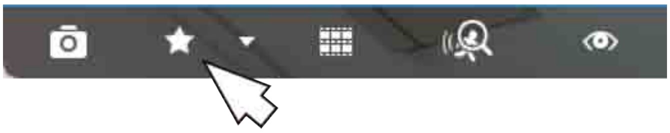
Item	QTY	Price
HARIBO GOLDBEARS	1	9.99

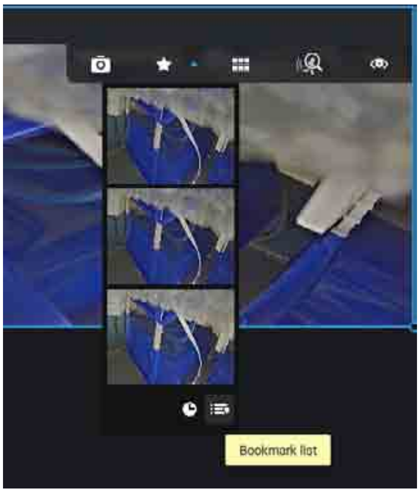
Total: 9.99

Payment: 10

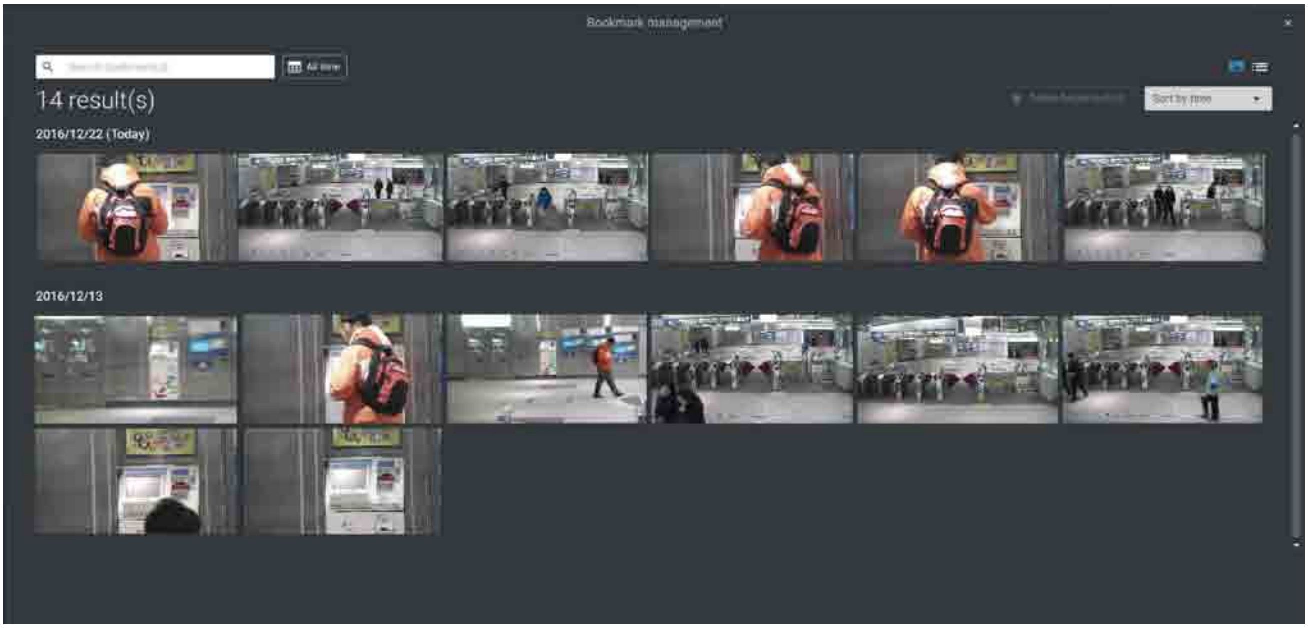
Change: 0.01

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 when 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.

2-16. 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 both the **Liveview** and **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, 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 or Vehicle detection is selected, only objects detected as human or vehicle will be displayed as the search results.

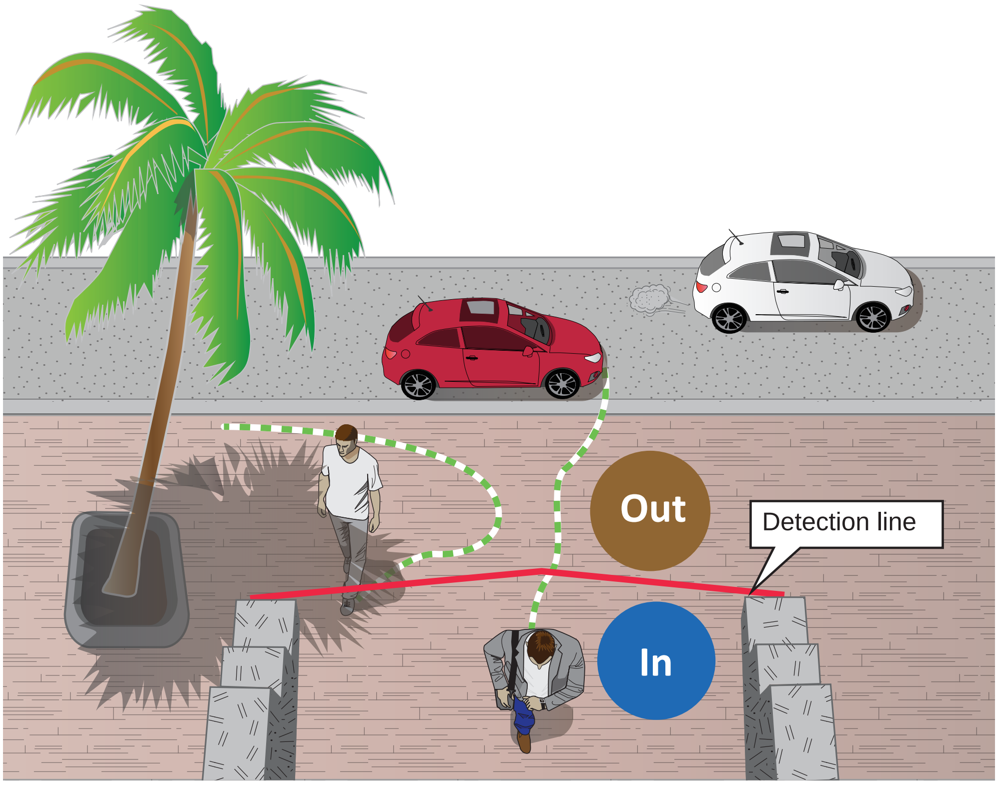
Please refer to VIVOTEK's website pages that are related to the Smart motion and Smart VCA features for the supported cameras.

Note that not all cameras support the latest vehicle detection feature.

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

Line Crossing Detection

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



The applicable scenarios of this feature can be:

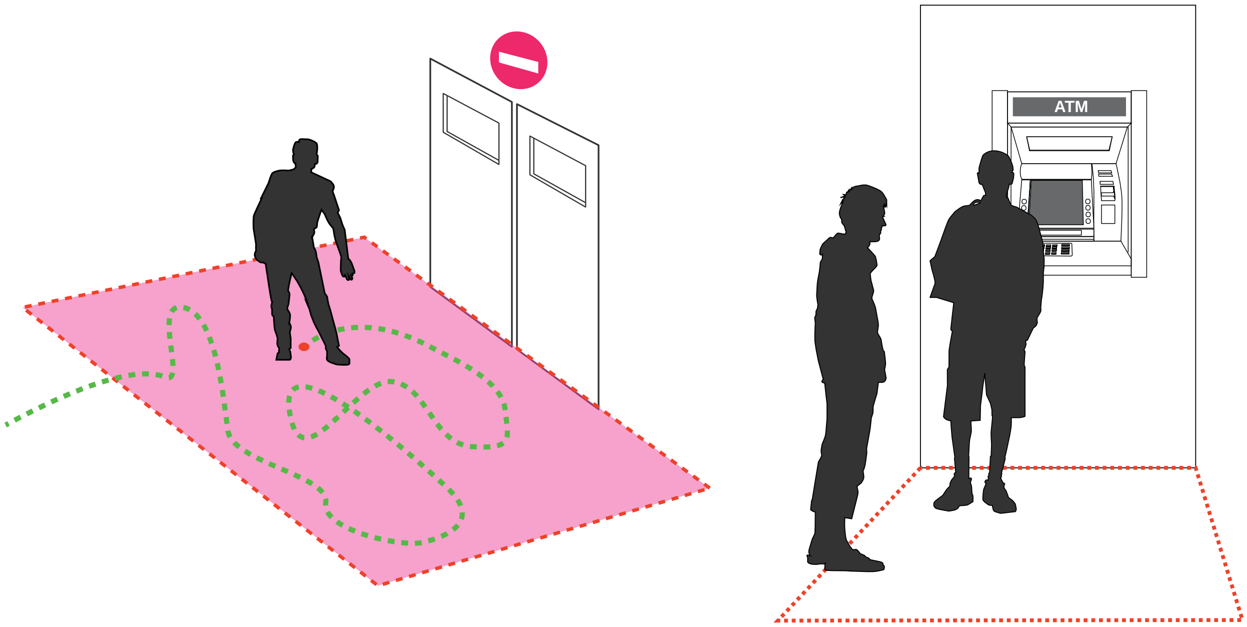
* Detects someone who enters a drive way, entrance, or exit through the virtual line.

* Detects and triggers an alarm in a predetermined direction.

* The detection line can be used as a fence boundary to know if someone has crossed the articulated line around a perimeter.

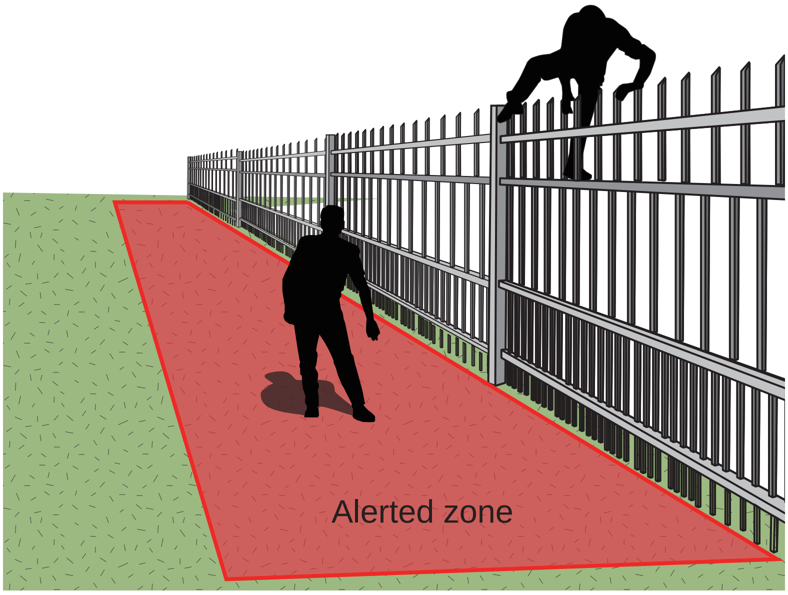
Loitering Detection

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



Intrusion Detection

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



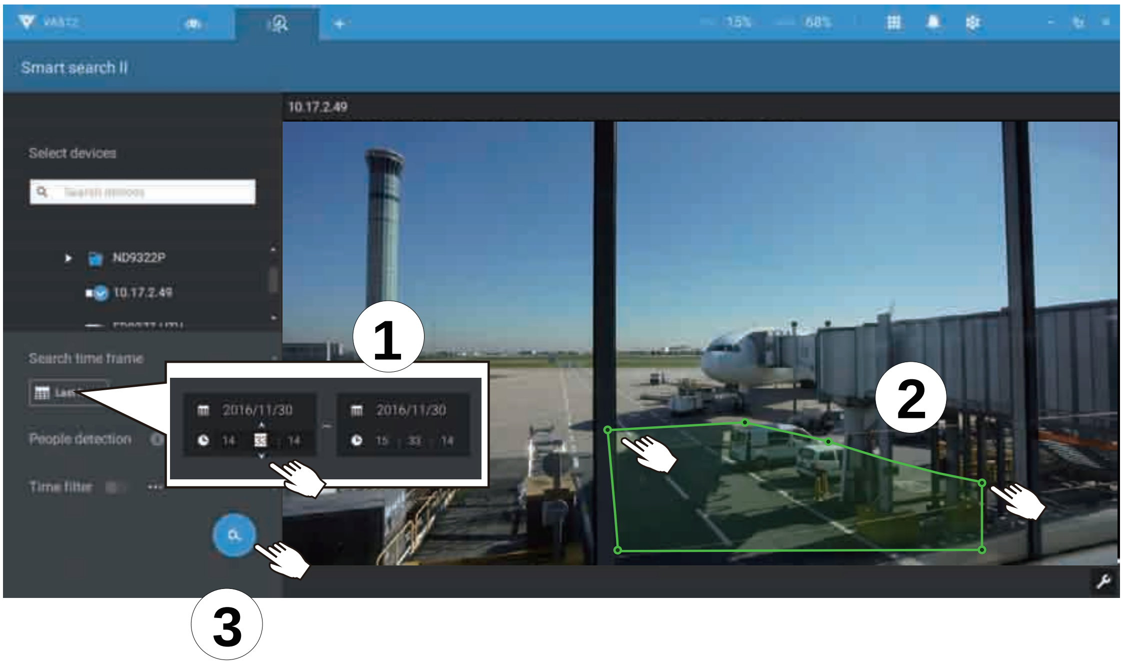
The applicable scenarios of this feature can be:

* Detects when a person enters a bank vault or school after the office hours.

* Detects when a person leaves an emergency exit or fire escape, or any place that is normally forbidden from access.

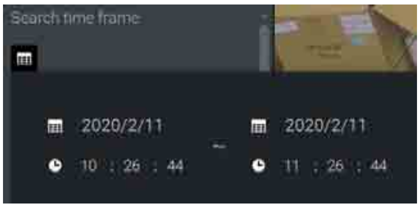
To use Smart search,

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



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

Search parameters:

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

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

IMPORTANT:

Running Smart Search II requires cameras that support the following:

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

NOTE:

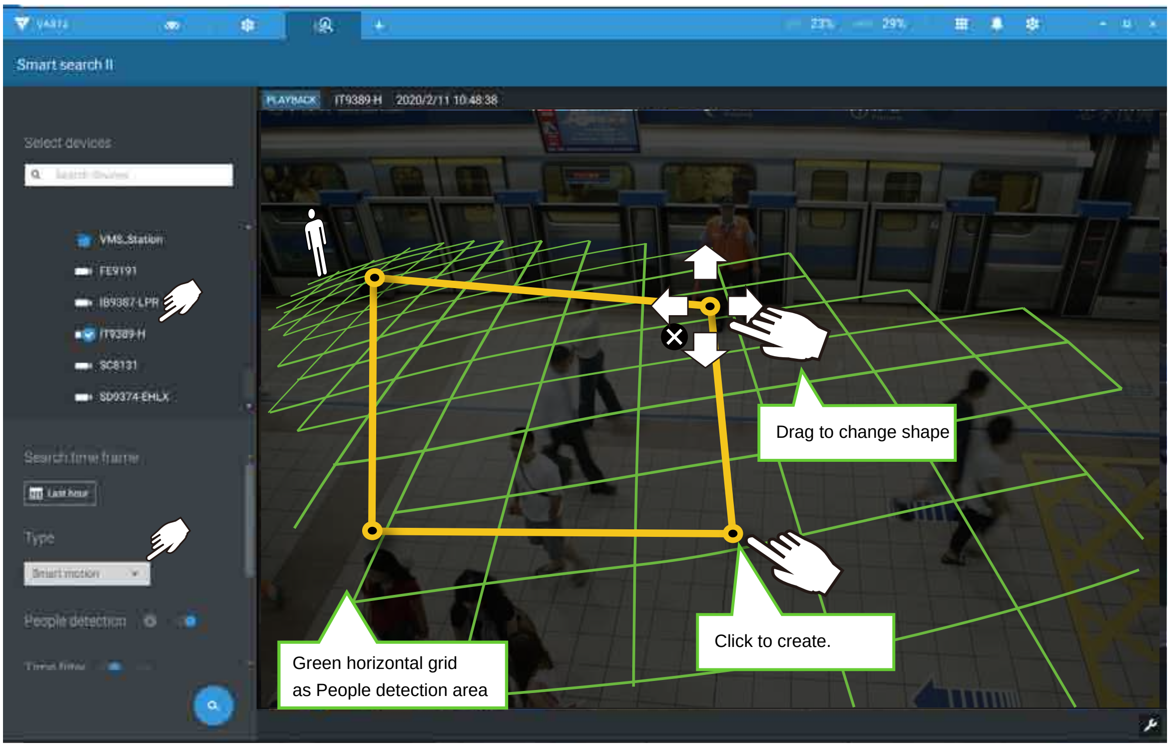
* Smart search II supports people detection whether the camera comes with a Smart motion license or not. However, the Line crossing, Loitering, Intrusion features will not be available.

* With a valid VCA package and license, the abovementioned features will be available in the Smart search II.

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

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

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



Drag to change shape

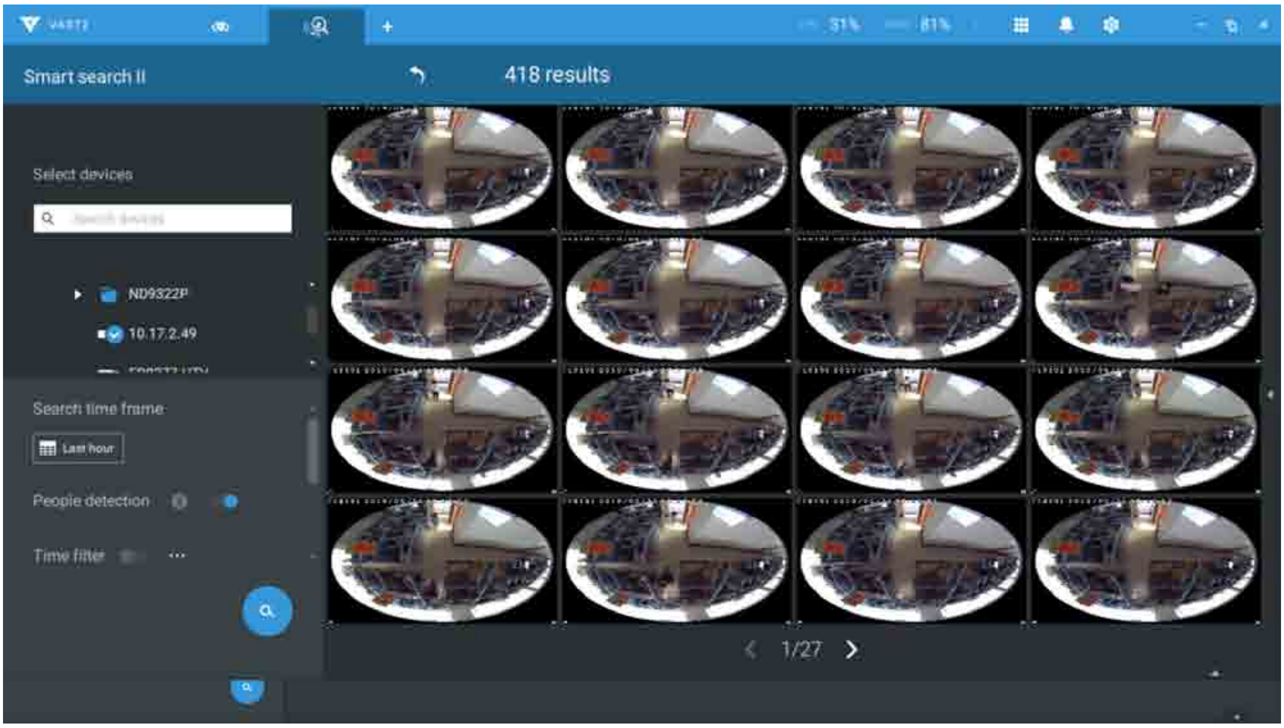
Click to create.

Green horizontal grid as People detection area

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

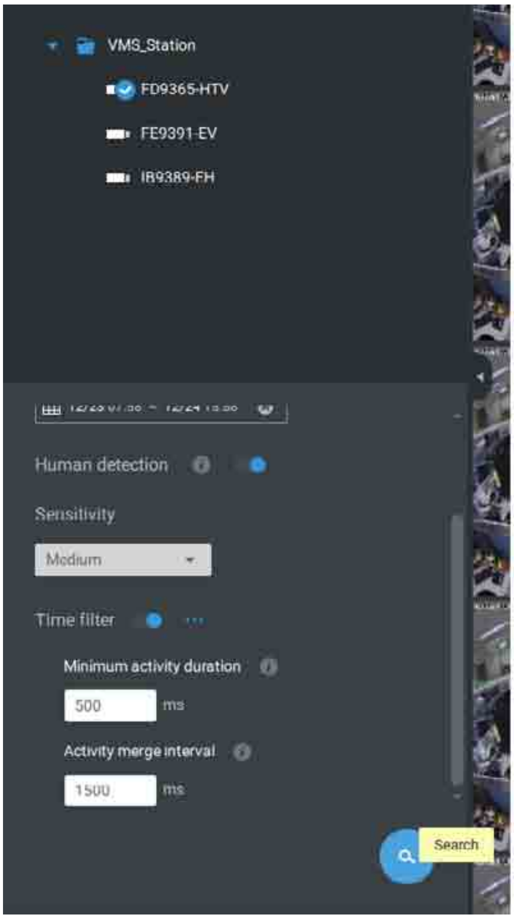
   Hover the screen with your mouse, and the length of each video clip is displayed.

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



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

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



Human detection

Sensitivity: Medium

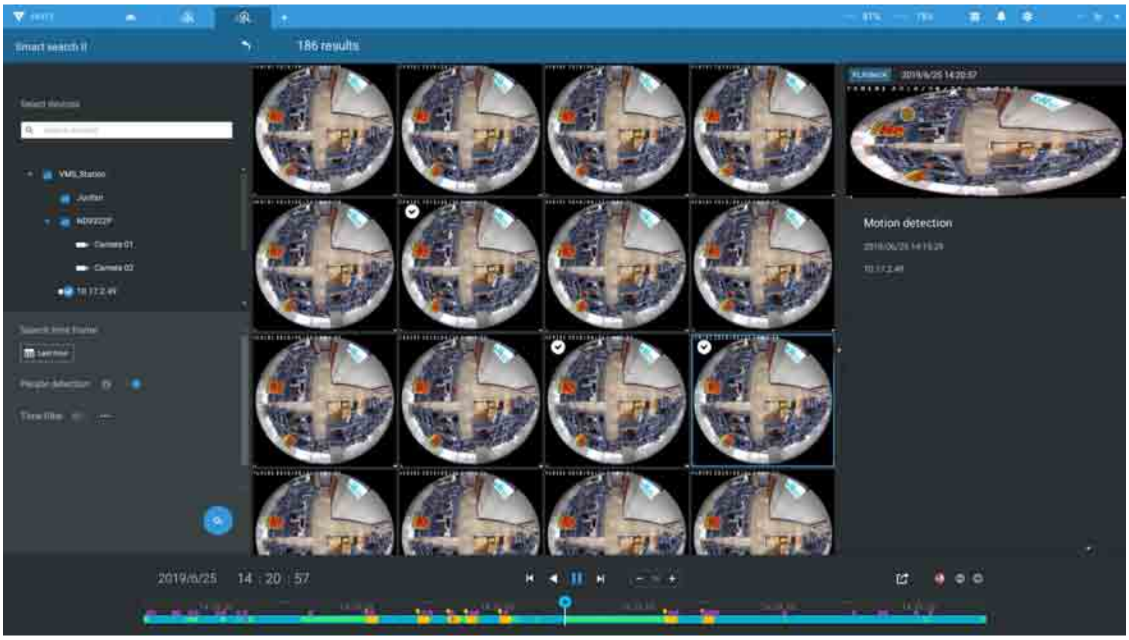
Time filter

Minimum activity duration: 500 ms

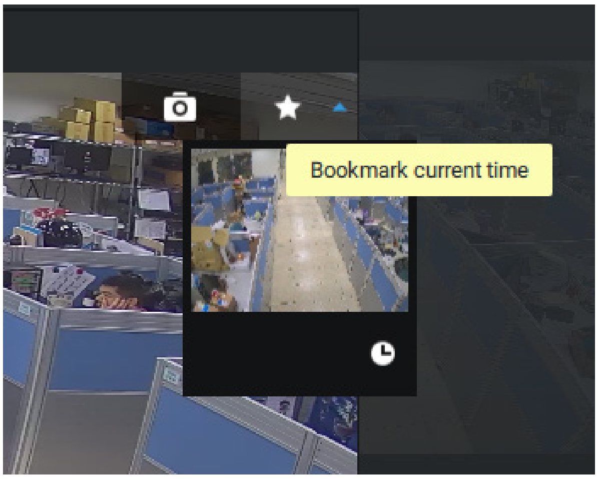
Activity merge interval: 1500 ms

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

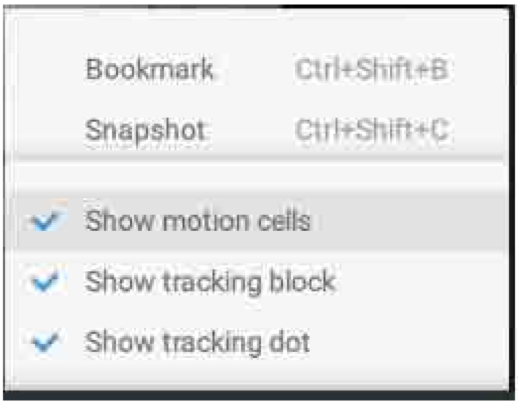
5. You can then click to open any clip of your interest. Each marked event clip will be indicated by a lighter color on the time line. Select and double-click on a video clip, and then right-click or select the bookmark or snapshot functions from the upper-right.



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



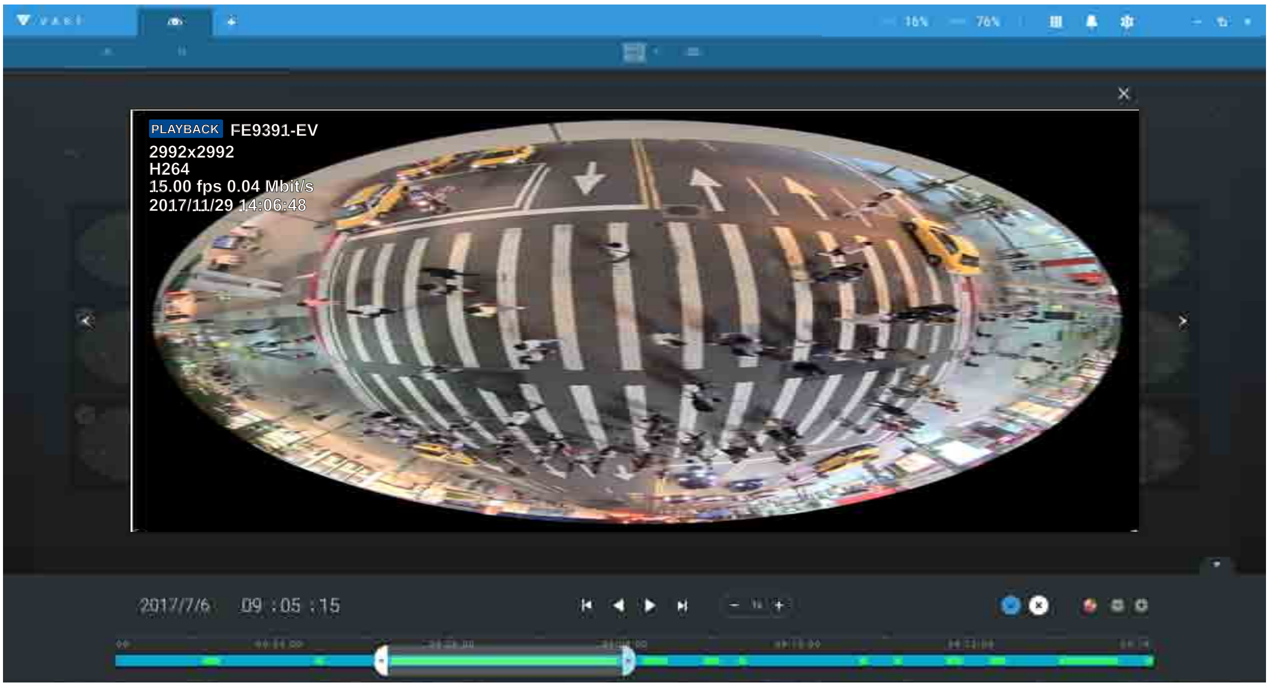
While in the full-screen Playback window, you can right-click to select or deselect the display elements including motion cells, tracking block, and tracking dot.



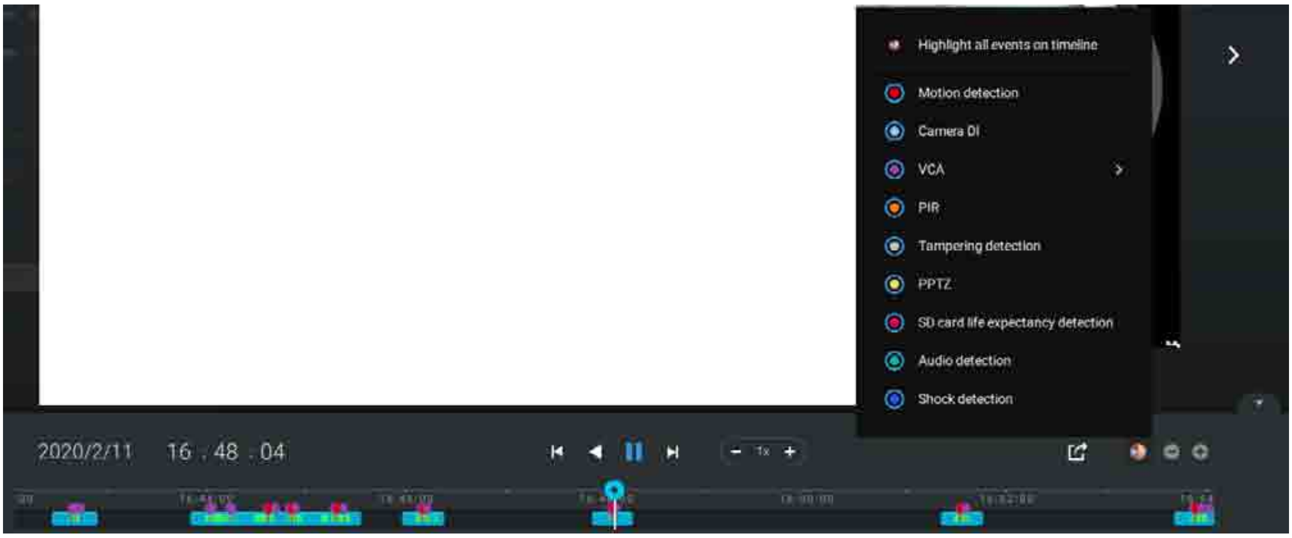
Bookmark Ctrl+Shift+B
Snapshot Ctrl+Shift+C
✓ Show motion cells
✓ Show tracking block
✓ Show tracking dot

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.



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

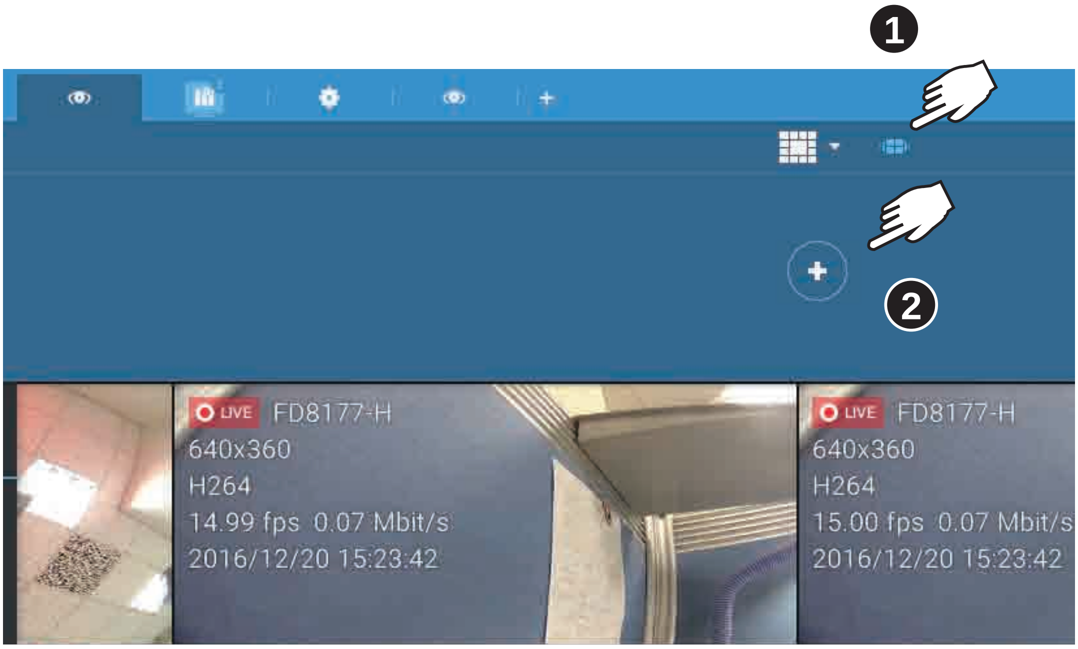


2-17. Tour

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,

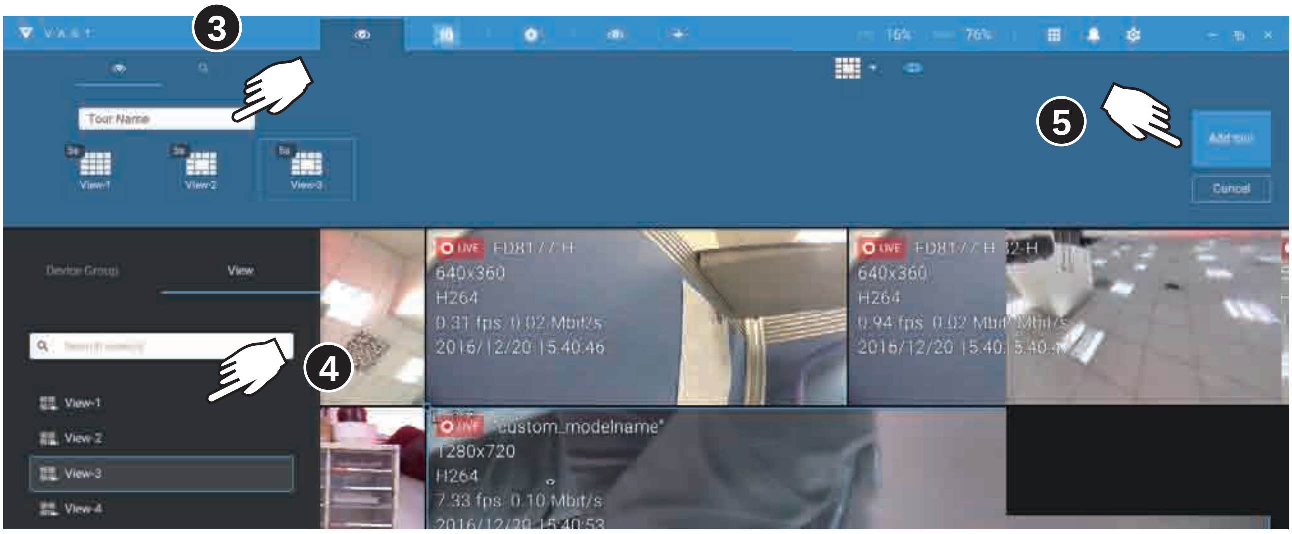
1. Click on the Add a camera tour button.
2. Click the Add button.



FD8177-H
640x360
H264
14.99 fps 0.07 Mbit/s
2016/12/20 15:23:42

FD8177-H
640x360
H264
15.00 fps 0.07 Mbit/s
2016/12/20 15:23:42

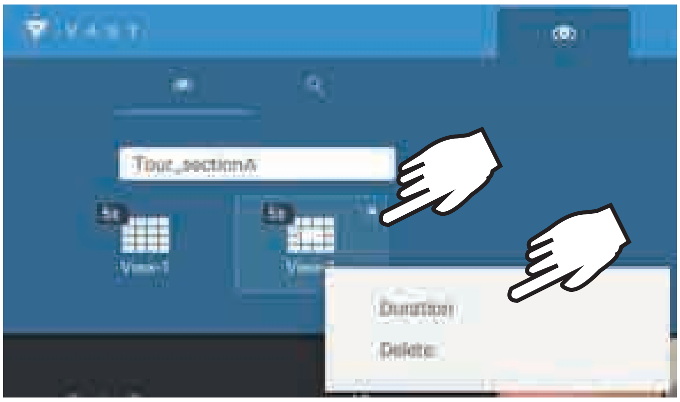
3. Enter a name for the tour.
4. Single-click to select a view. Select multiple views each by a single click.
5. Click the Add Tour button.



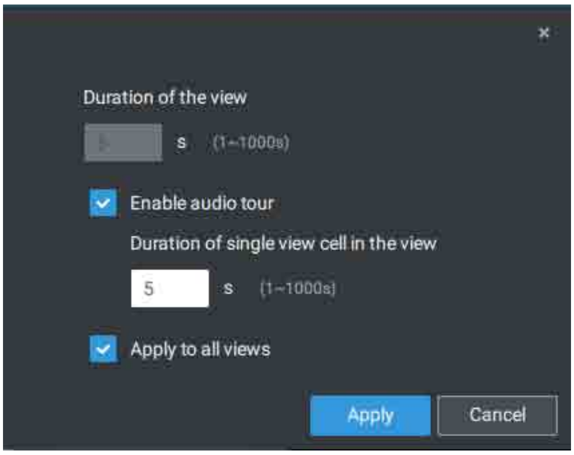
FD8177-H
640x360
H264
0.31 fps 0.02 Mbit/s
2016/12/20 15:40:46

custom_modelname
1280x720
H264
7.33 fps 0.10 Mbit/s

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



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



Duration of the view

5 s (1~1000s)

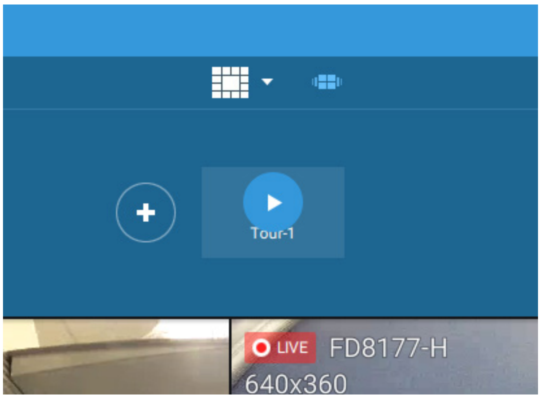
☑ Enable audio tour

Duration of single view cell in the view

5 s (1~1000s)

☑ Apply to all views

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.

2-18. Thumbnail search

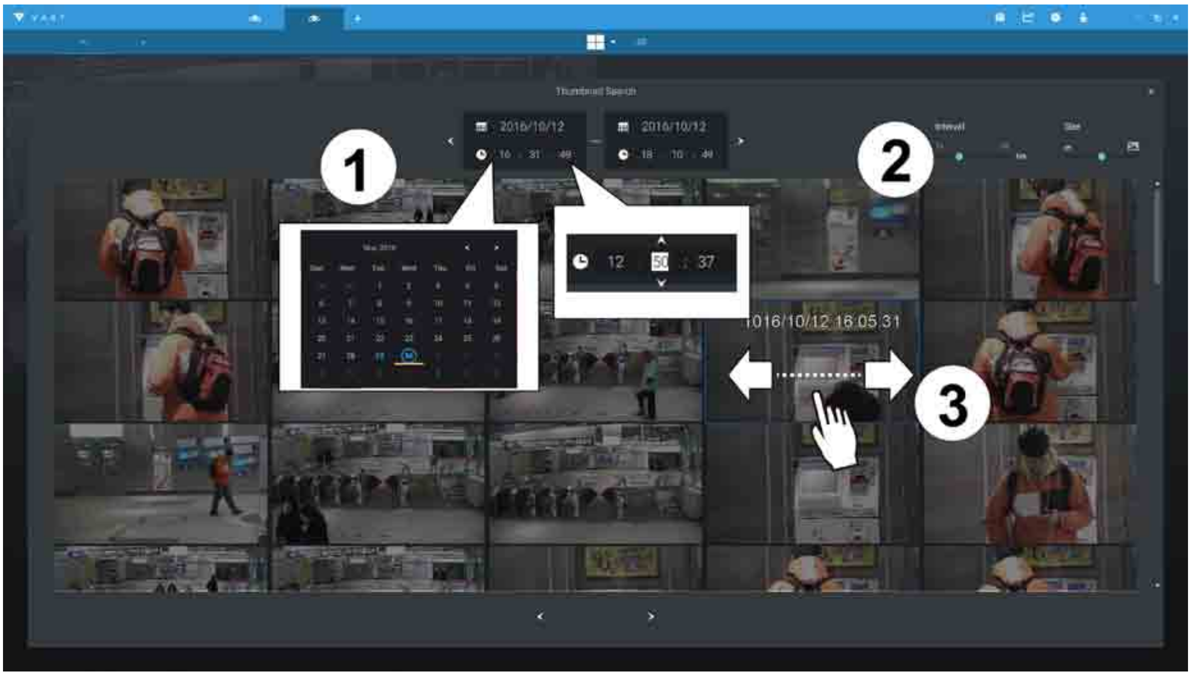
The Thumbnail search function is like doing a post-production editing in film making. Screens from across different time spans are shown to facilitate the search for evidence.

VAST now supports the search for the instances stored on VIVOTEK's Linux-based NVRs.

Click on the Thumbnail search 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,

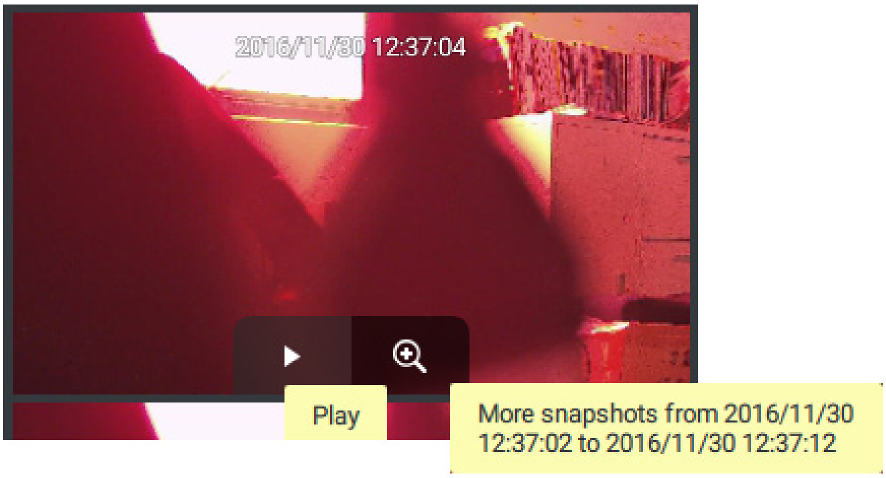
1. Use the date and time selectors to specify a time span during which you suspect the event of your interest has occurred.
2. If preferred, tune the interval and clip size. The default length for each clip is 10 seconds.
3. If you find a clip might contain an event of your interest, you can click to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

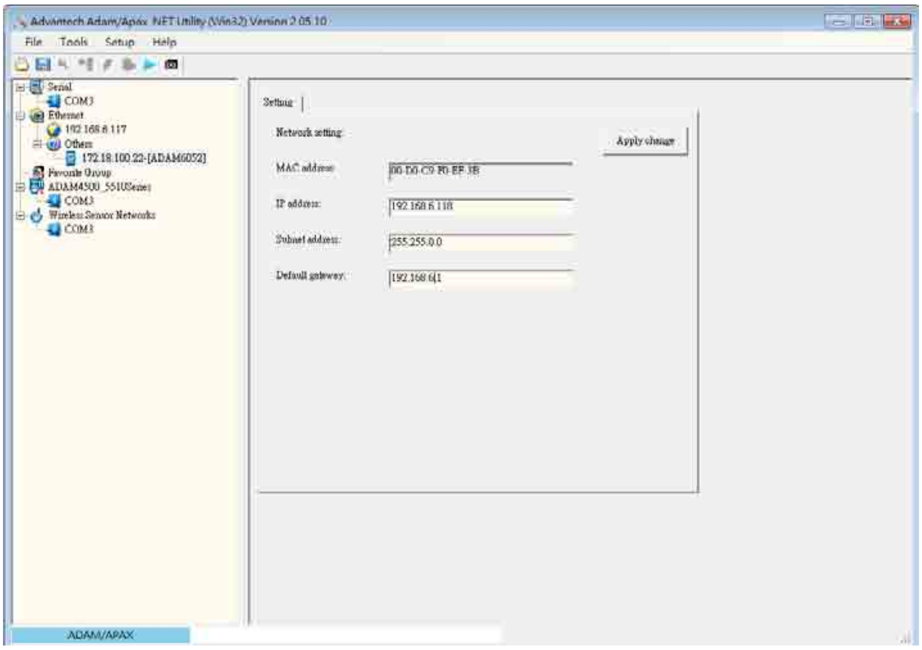

2016/11/30 12:37:04
Play
More snapshots from 2016/11/30 12:37:02 to 2016/11/30 12:37:12

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.



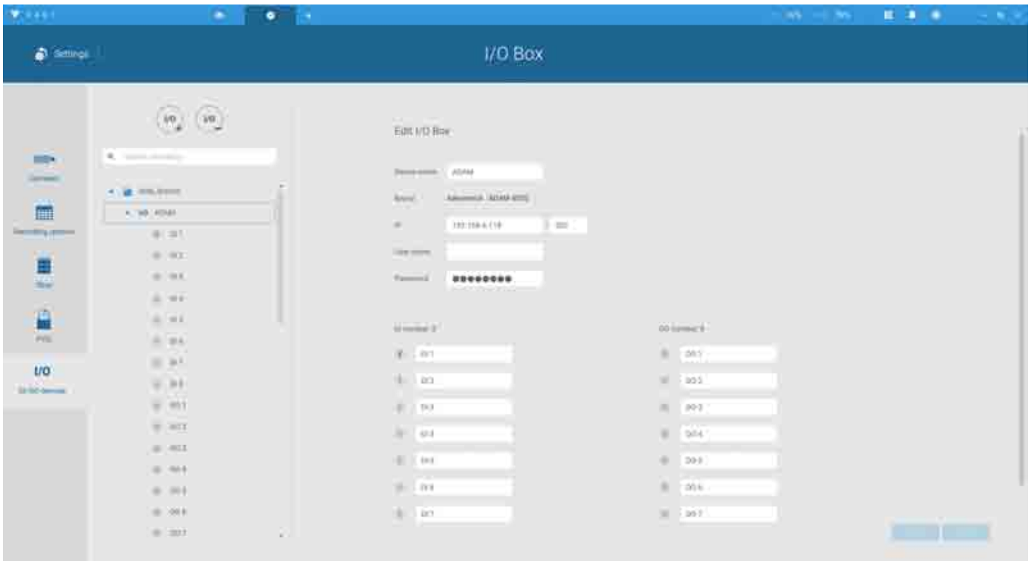
MAC address: 00-D0-C9-F0-EF-3B

IP address: 192.168.6.118

Subnet address: 255.255.0.0

Default gateway: 192.168.6.1

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

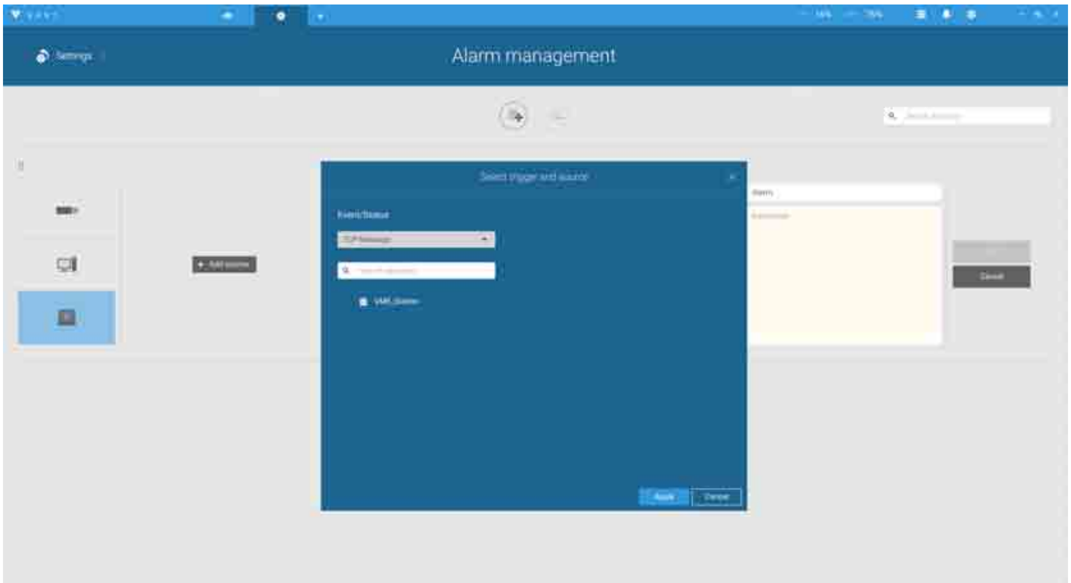


Enter the I/O box's IP addess and credentials, and select the correct model name from the pull-down list on the right. Click the **Apply** button to proceed. The current I/O connections are also displayed on screen, such that the status is displayed when DI pins are connected to detection devices.

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

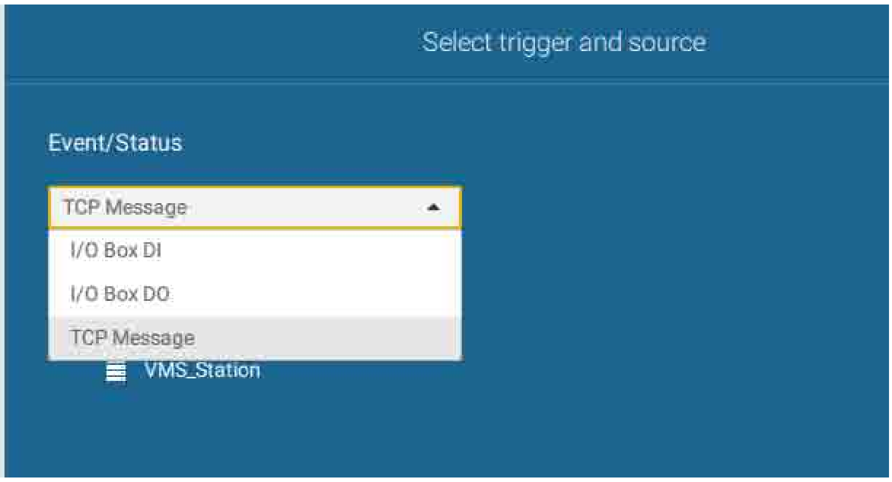
Enter the **Settings** > **Alarm** window. Click the **Add alarm** button on top.

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

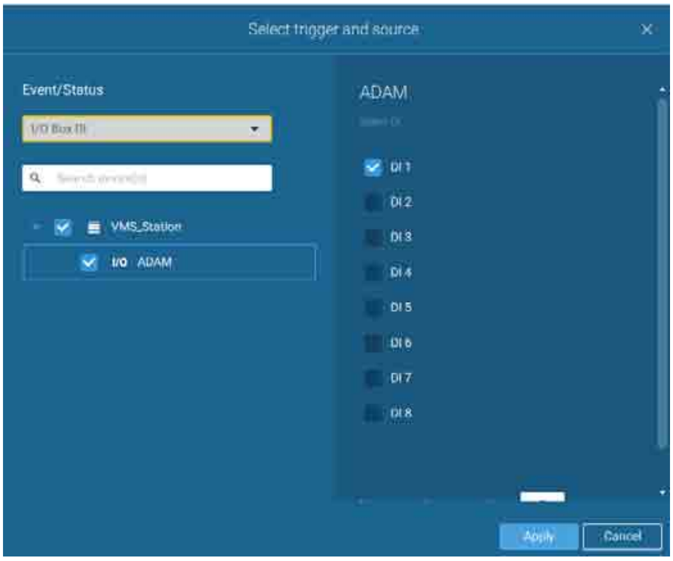


The **Select trigger and source** window will prompt.

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.



Select trigger and source

Event/Status: I/O Box DI

Search device(s)

☑ VMS_Station
☑ I/O ADAM

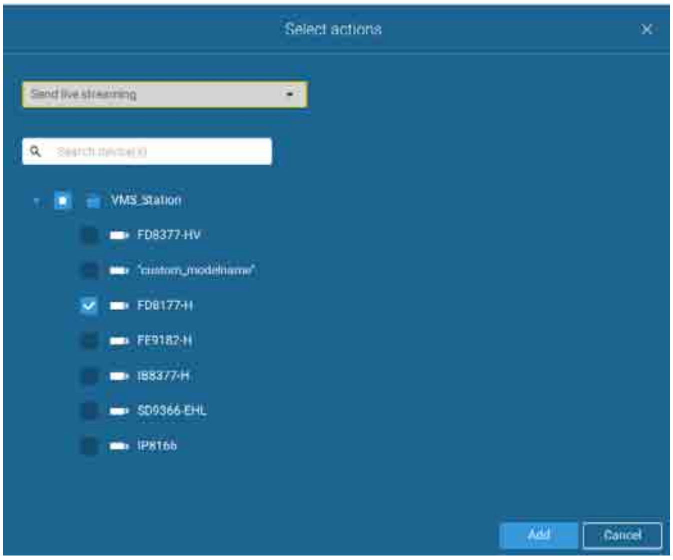
ADAM

Select DI

☑ DI 1
□ DI 2
□ DI 3
□ DI 4
□ DI 5
□ DI 6
□ DI 7
□ DI 8

Apply | Cancel

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



Select actions

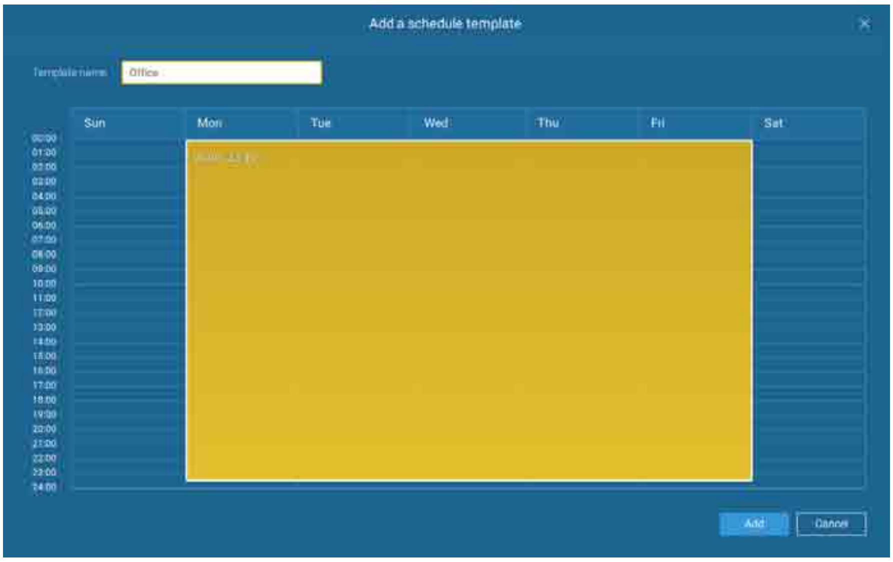
Send live streaming

Search device(s)

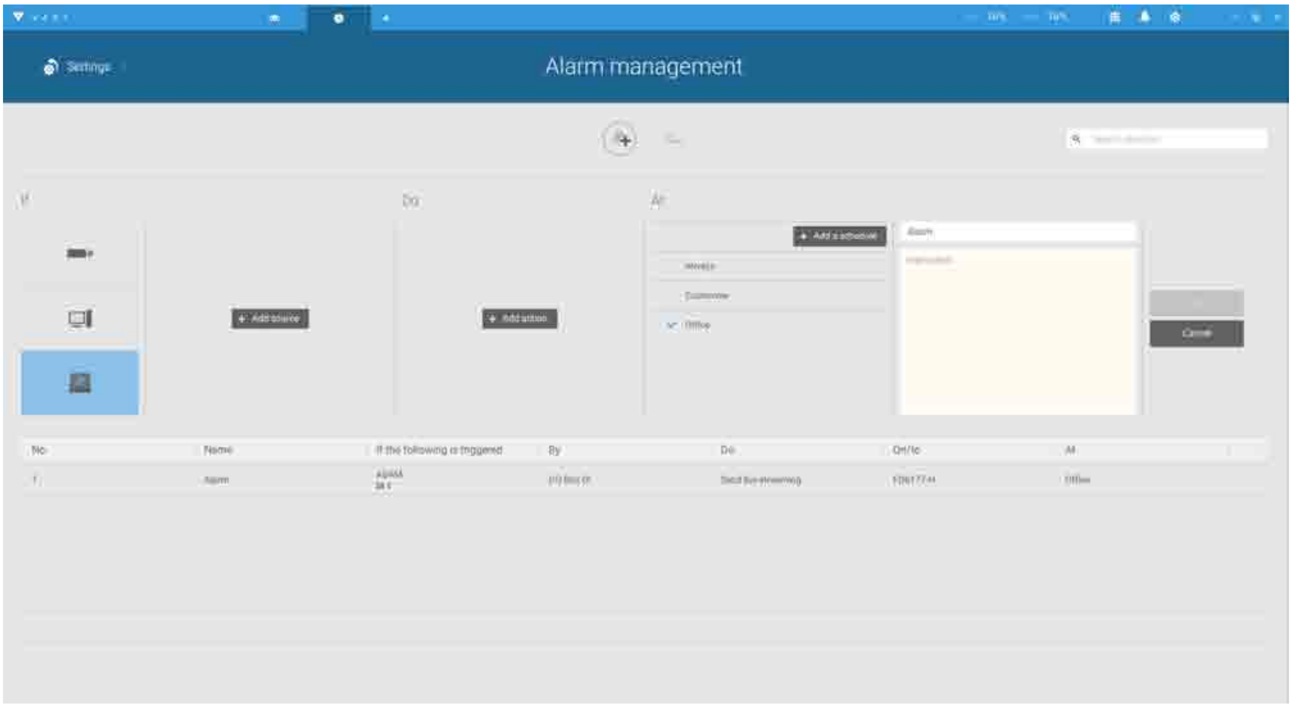
■ VMS_Station
□ FD8377-HV
□ "custom_modelname"
☑ FD8177-H
□ FE9182-H
□ IB8377-H
□ SD9366-EHL
□ IP8166

Add | Cancel

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

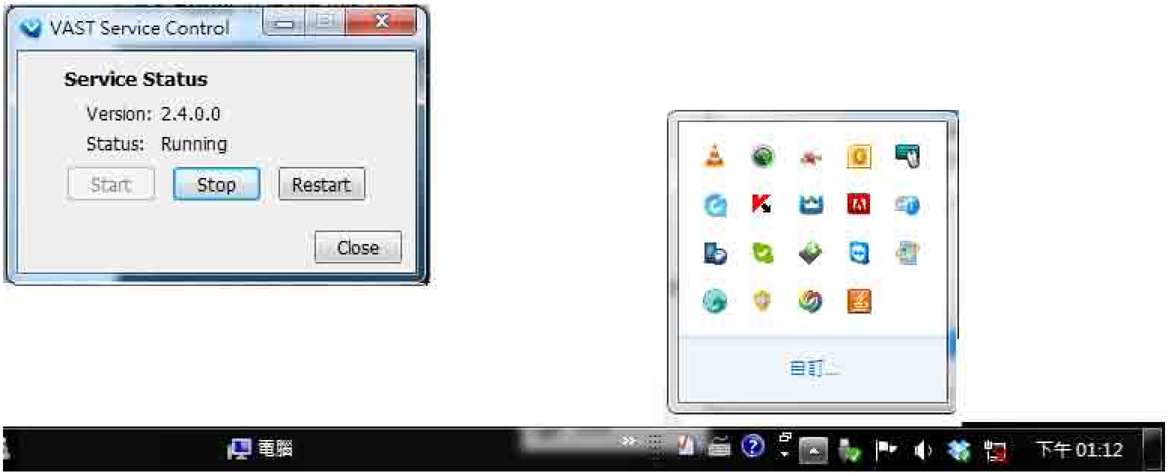


Enter a name for your Alarm, and add description for your configuration, e.g., "intrusion detected on the front door." When done, click the **Add** button. The Alarm configuration takes effect immediately.



No.	Name	If the following is triggered	By	Do	On/to	At
1	Alarm	[illegible]	[illegible]	Send live streaming	[illegible]	Office

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



VAST Service Control

Service Status

Version: 2.4.0.0

Status: Running

3-2. Configuring Redundant Servers - Failover

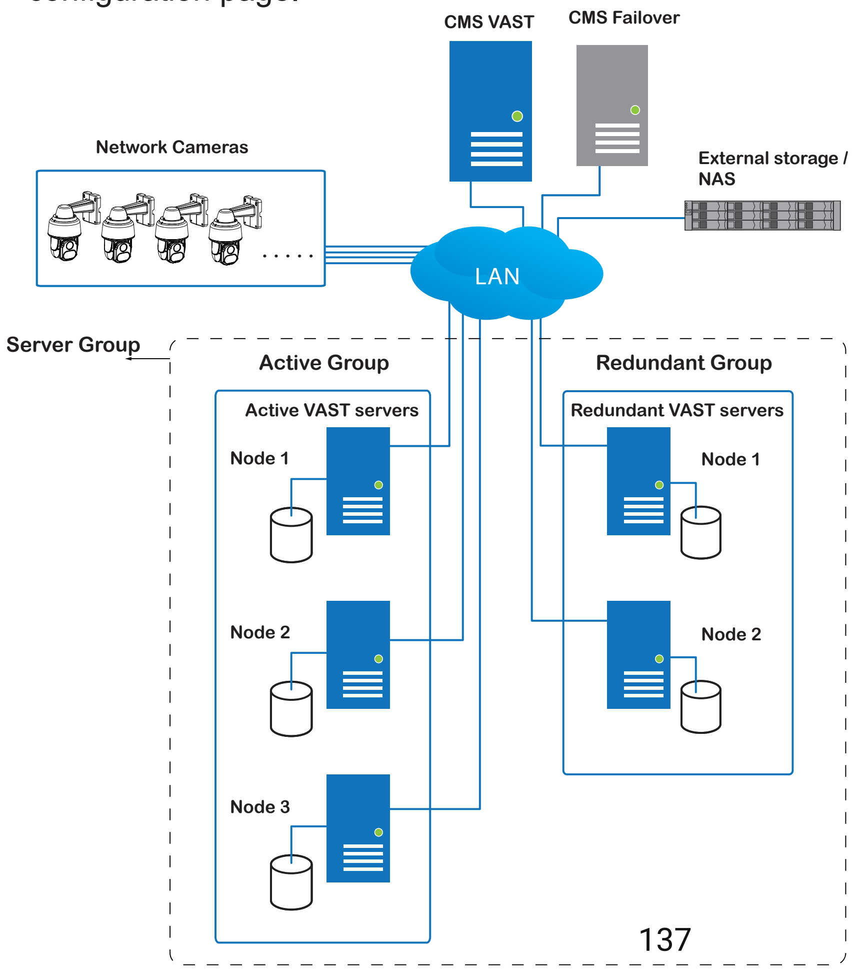
VAST2 servers can be configured into two groups: Active and Redundant. The Active group performs daily recording and monitoring tasks, while the Redundant group acts as the standby servers. In the event of server failures, the Redundant group becomes active, and takes over the recording task.

The Redundant server group configuration consists of the following:

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

IMPORTANT:

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



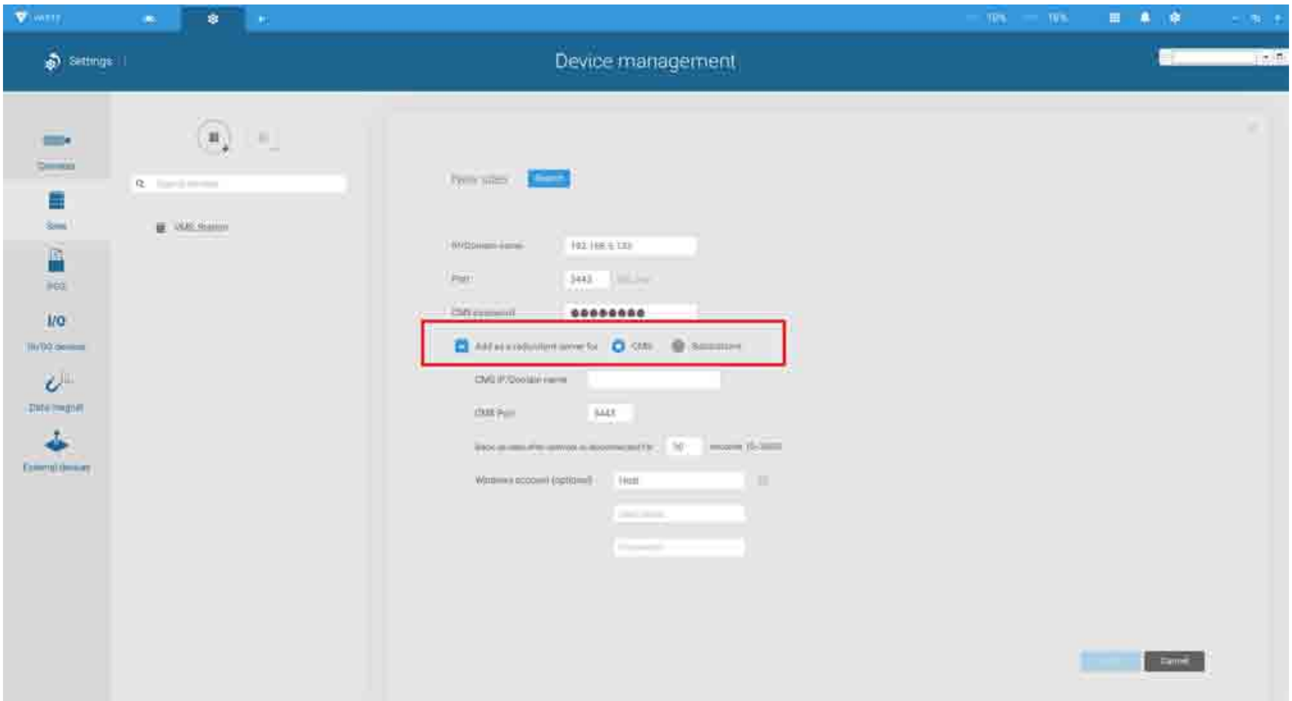
Below are the definitions of server roles:

1. **CMS** VAST server: The main access portal for the configuration.

1-1.	CMS server is where the **Failover** configuration takes place.
1-2.	CMS continuously polls to check the hearbeats to monitor the statuses of all Active and Redundant servers.
1-3.	CMS regularly backs up the configurations on Active servers.
1-4.	CMS assigns redundant server(s) to the takeover of a failed Active server.
1-5.	In a Redundant server configuration, the CMS is supposed to be up and running at all time. If the CMS server fails, the server failover and failback operation will not take place. It is therefore preferrable to configure a CMS redundant server, and install the CMS server at a high up-time environment, such as on a VMWare configuration.

2. **CMS Redundant** server: This is a failover server that serves as the backup for the CMS server.

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



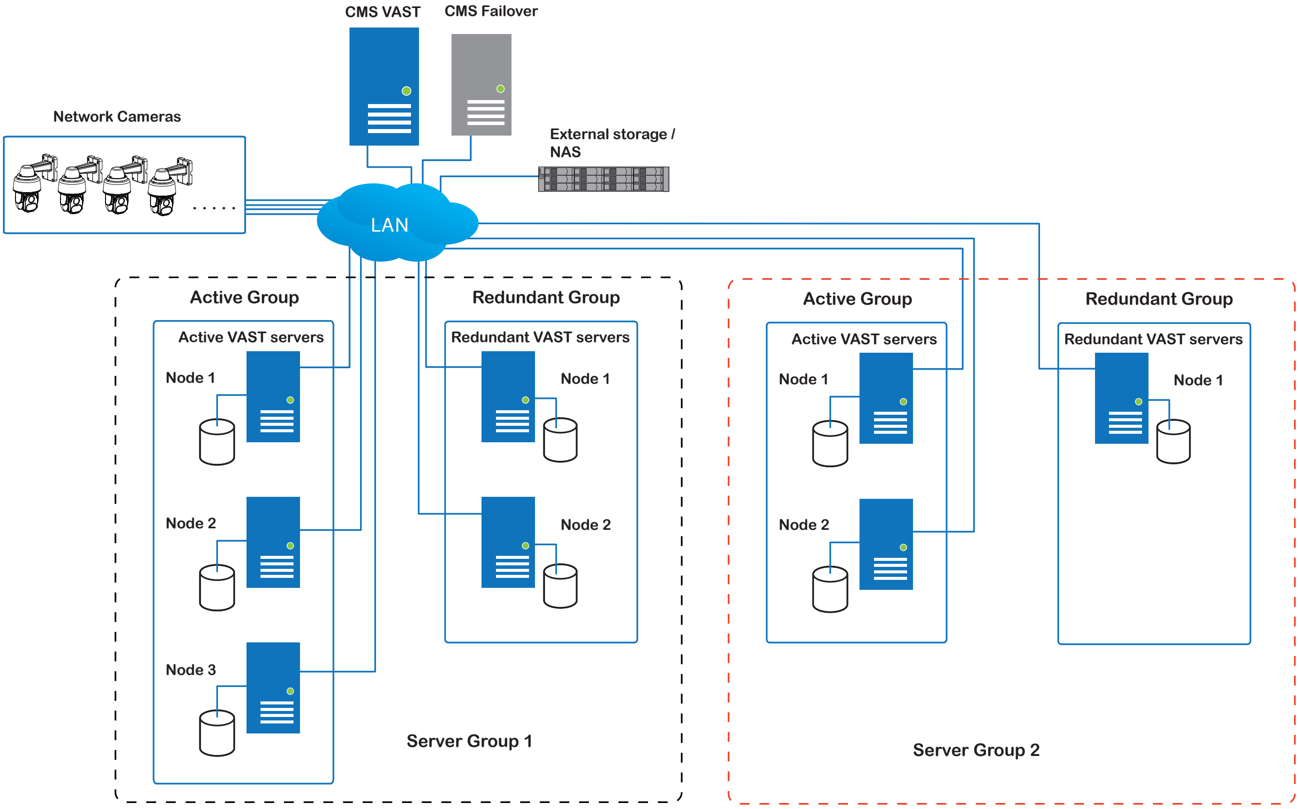
IP/Domain name: 192.168.5.130
Port: 3443
CMS password: ●●●●●●●●
☑ Add as a redundant server for ● CMS ○ Substation
CMS IP/Domain name:
CMS Port: 3443
Windows account (optional): Host

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

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

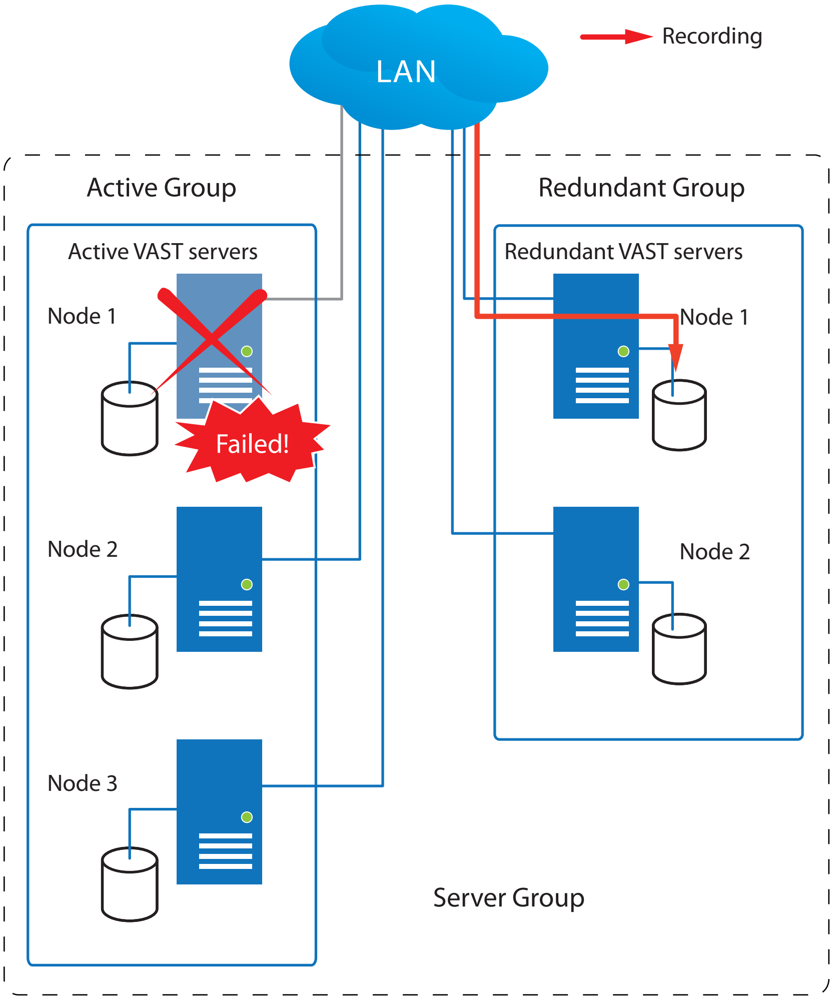
The conditions during the failover process are illustrated below:

Multiple Active and Redundant groups can be created.

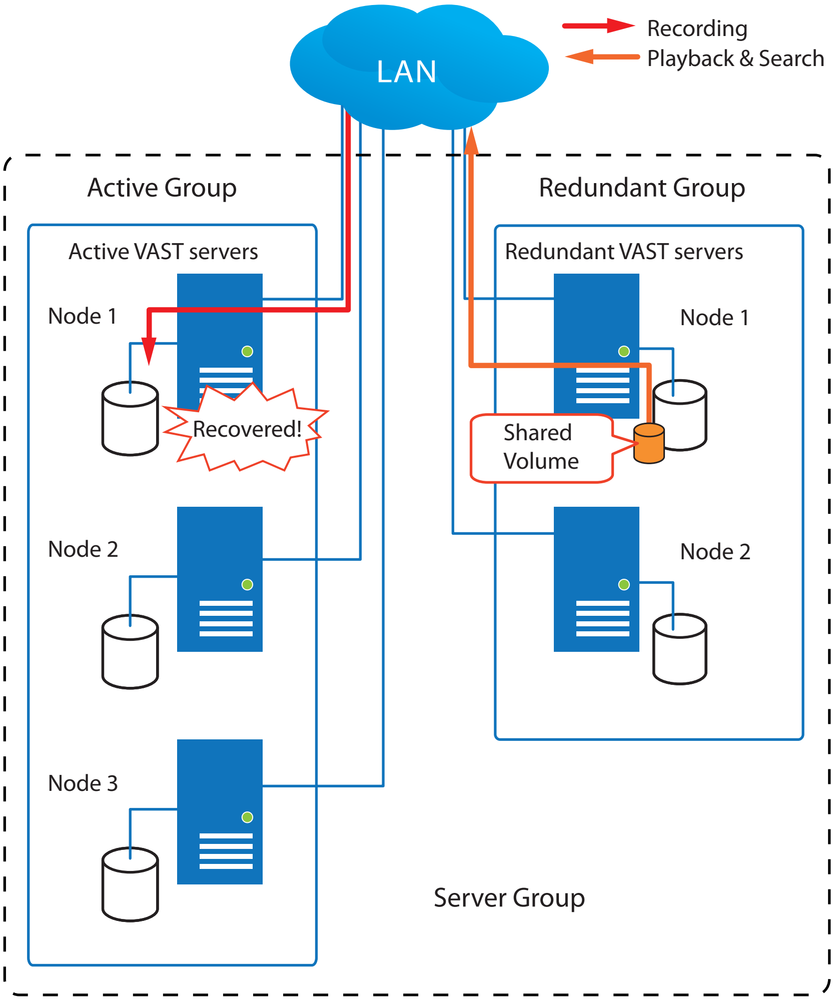


Each Redundant server can serve as the backup for ONE Active server. Depending on the number of the Active and Redundant servers, if the number of failed servers exceeds the number of Redundant servers, the failover will be abandoned. For example, if 2 Active servers failed, and there is only 1 Redundant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

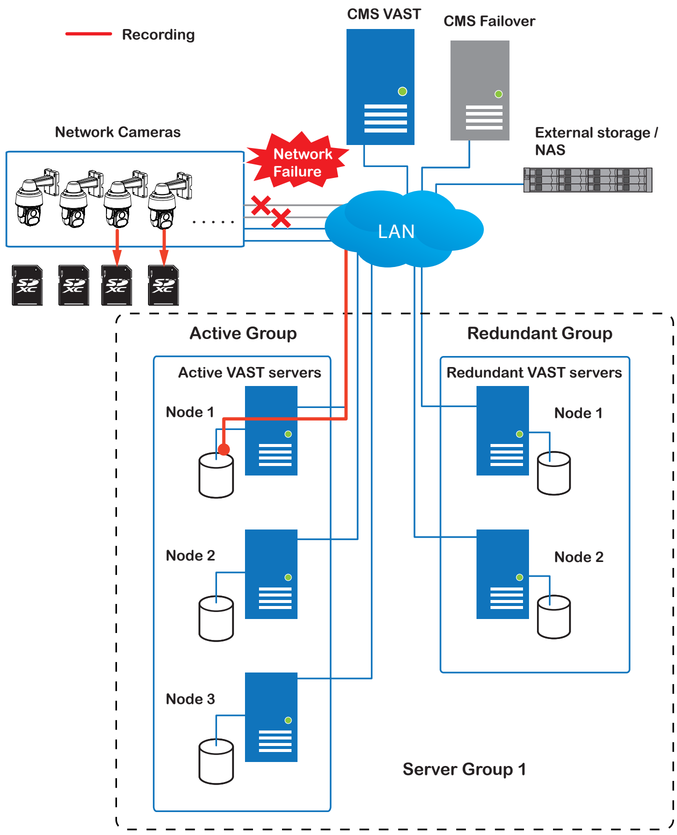
In the event of a server failover, a VAST2 server in the Redundant group takes over the recording task. Note that depending on the network environment, the takeover can take up to 5 minutes.



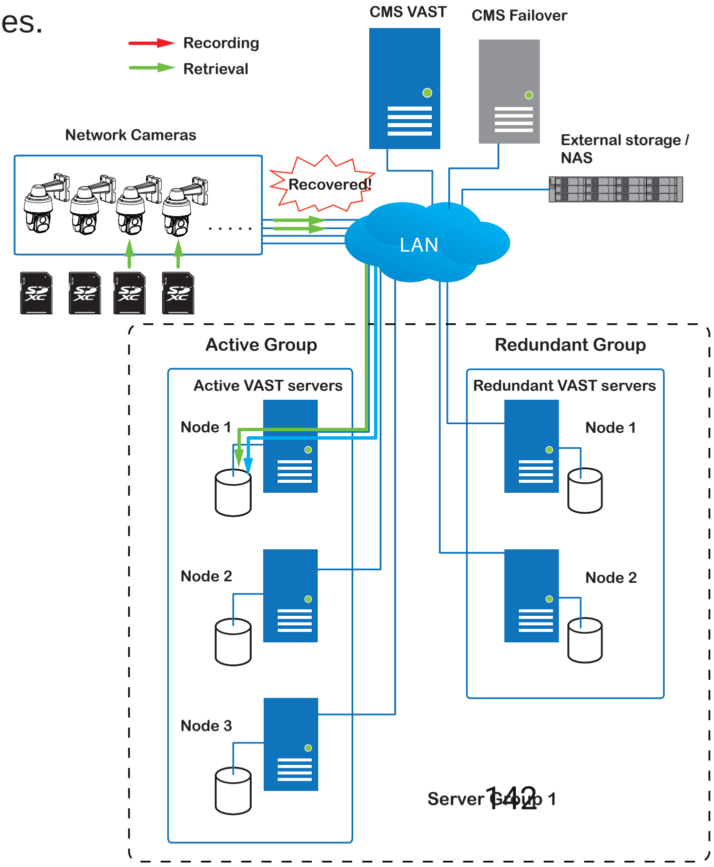
Once the server in the Active group is restored to normal operation, and a CMS server requests for the recordings and data occurred during the time the active server failed, the requests will be fulfilled by a shared volume on the redundant server. Due to the concerns with network bandwidth and processing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



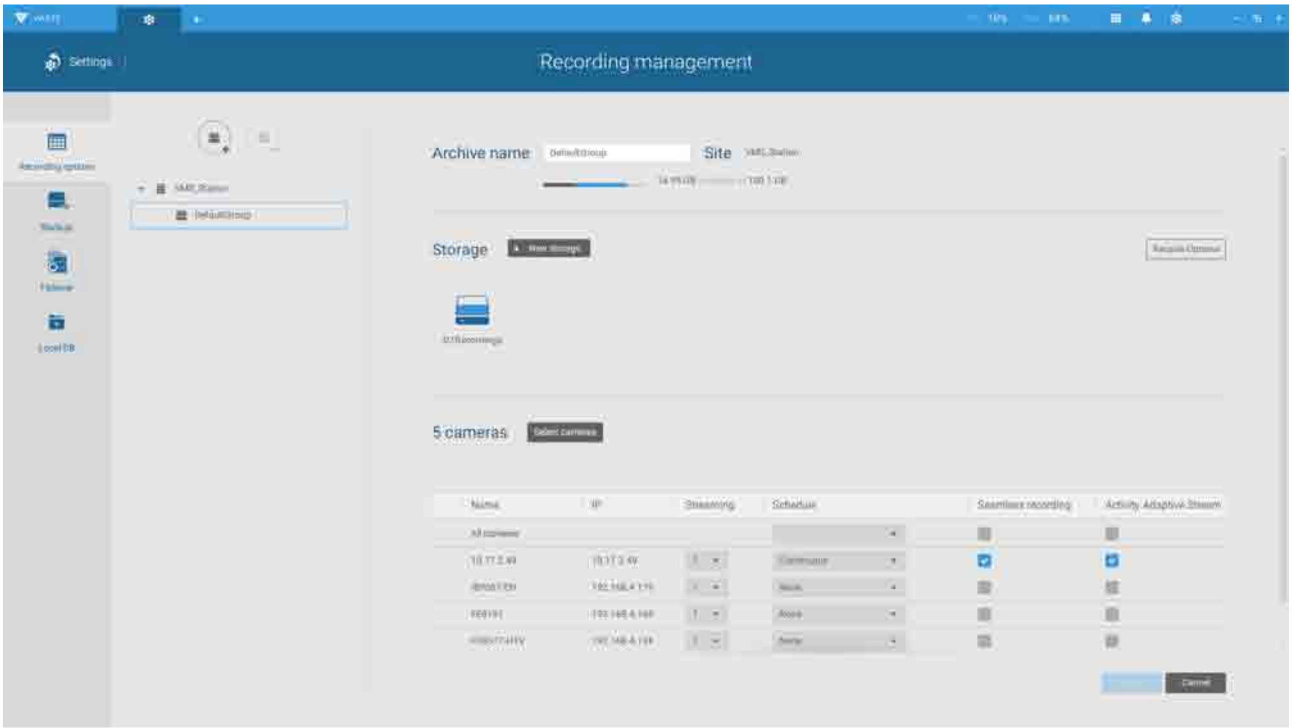
In terms of network failure, the VAST2 configuration supports Seamless Recording. For cameras equipped with an SD card, video is recorded to the SD cards in the event of network failure. Of course, the cameras must have a backup power source, such as a DC 12V input. In cases such as the only PoE switch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



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



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

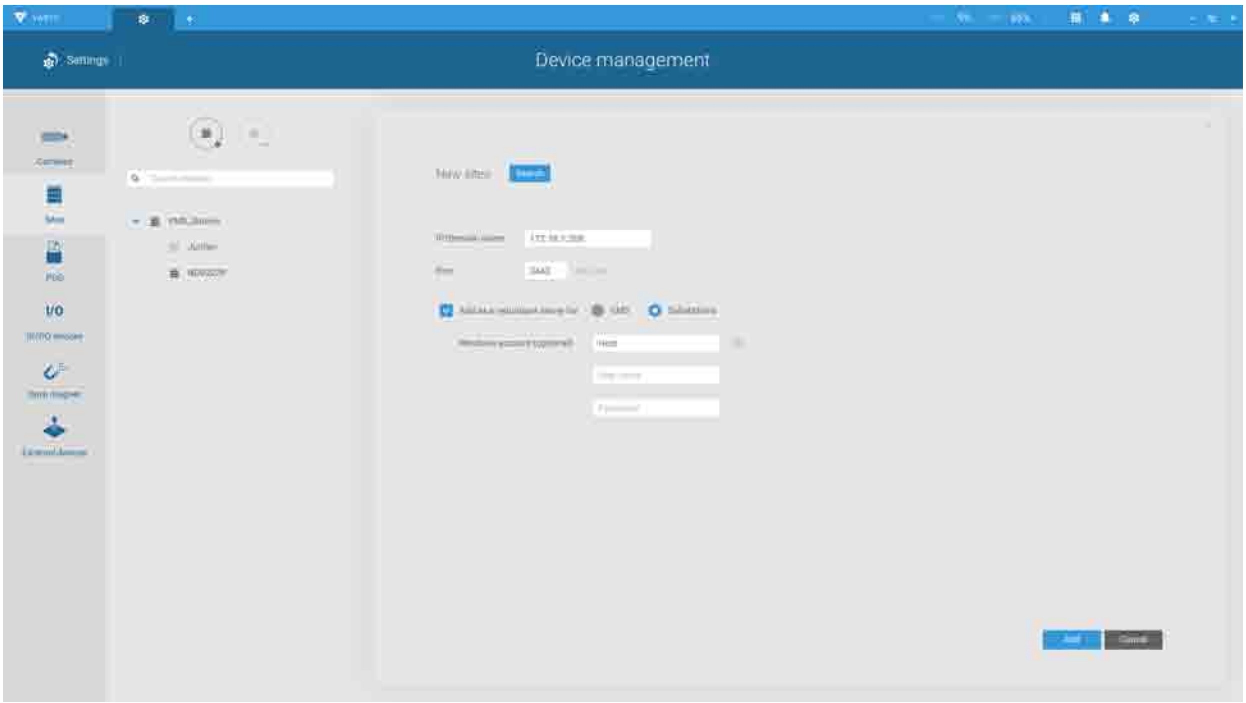


Name	IP	Streaming	Schedule	Seamless recording	Activity Adaptive Stream
All cameras				□	□
10.17.2.49	10.17.2.49	1	Continuous	☑	☑
[illegible]	192.168.4.175	1	None	□	□
FE8191	192.168.4.168	1	None	□	□
[illegible]	192.168.4.[illegible]	1	None	□	□

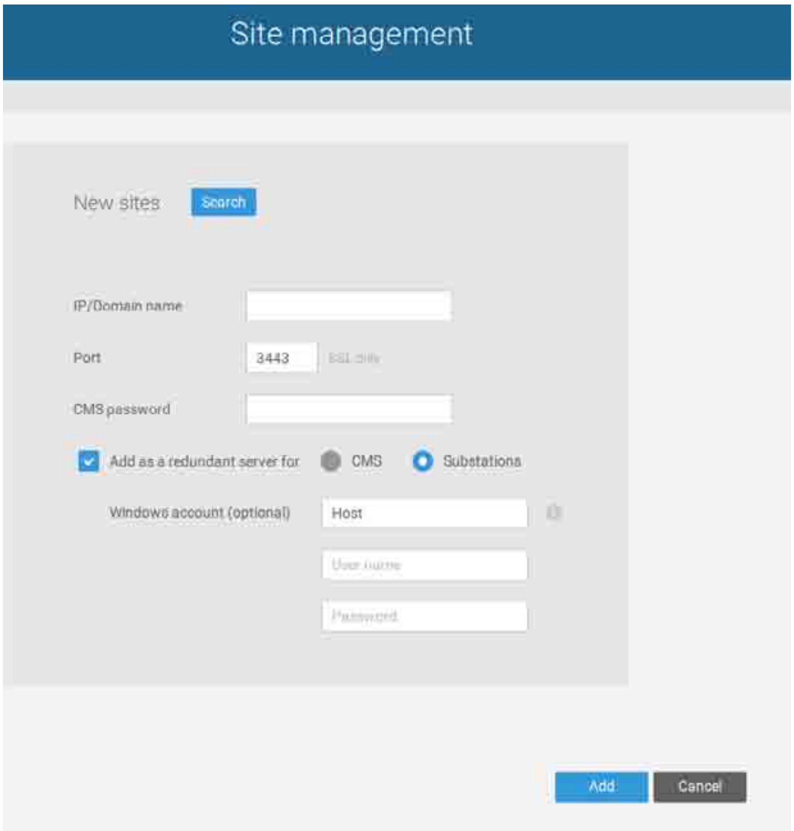
Failover Configuration Process

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

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



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



Site management

New sites

IP/Domain name

Port 3443 SSL only

CMS password

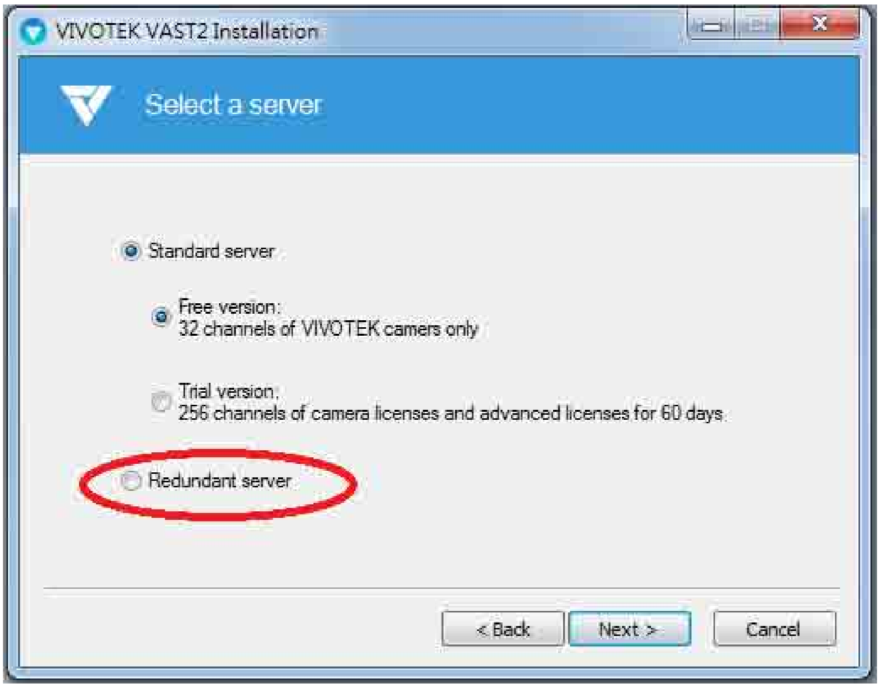
☑ Add as a redundant server for ○ CMS ● Substations

Windows account (optional) Host

User name

Password

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



VIVOTEK VAST2 Installation

Select a server

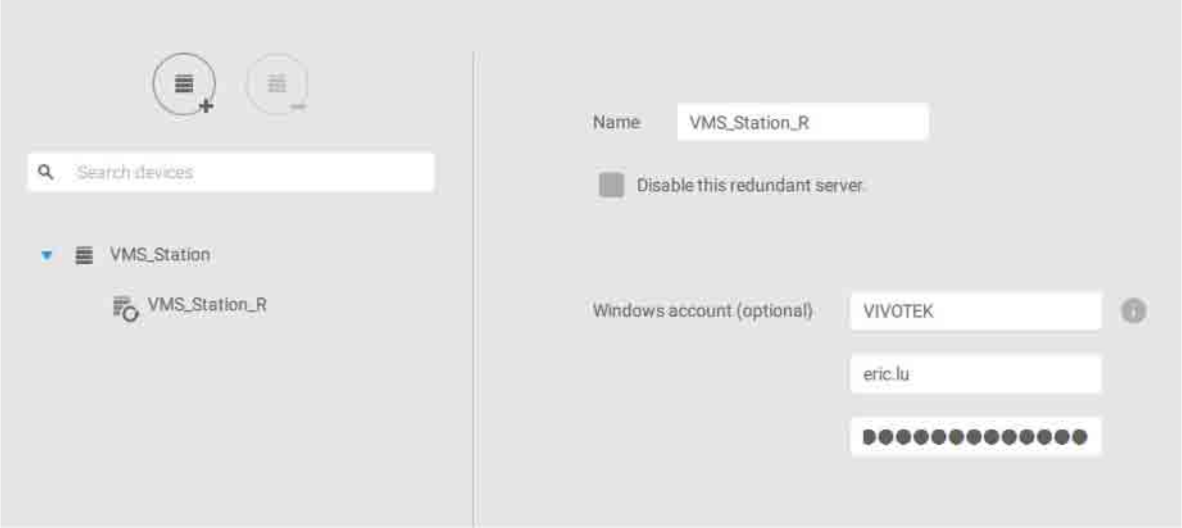
● Standard server

● Free version:
32 channels of VIVOTEK camera only

○ Trial version:
256 channels of camera licenses and advanced licenses for 60 days

○ Redundant server

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



Name: VMS_Station_R

□ Disable this redundant server

Windows account (optional): VIVOTEK

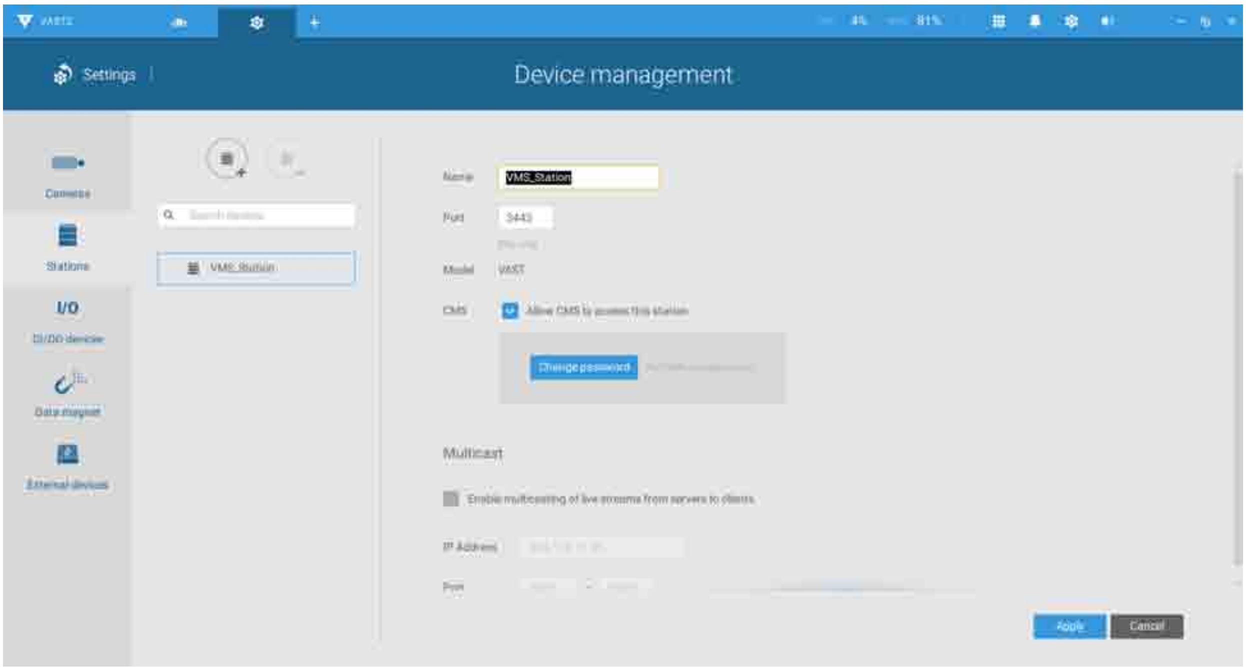
eric.lu

●●●●●●●●●●●●●●

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 Station management page, and select "**Allow CMS to access this station**." Create a common password for the CMS hierarchy.



Name: VMS_Station

Port: 3443

Model: VAST

CMS: ☑ Allow CMS to access this station

Multicast

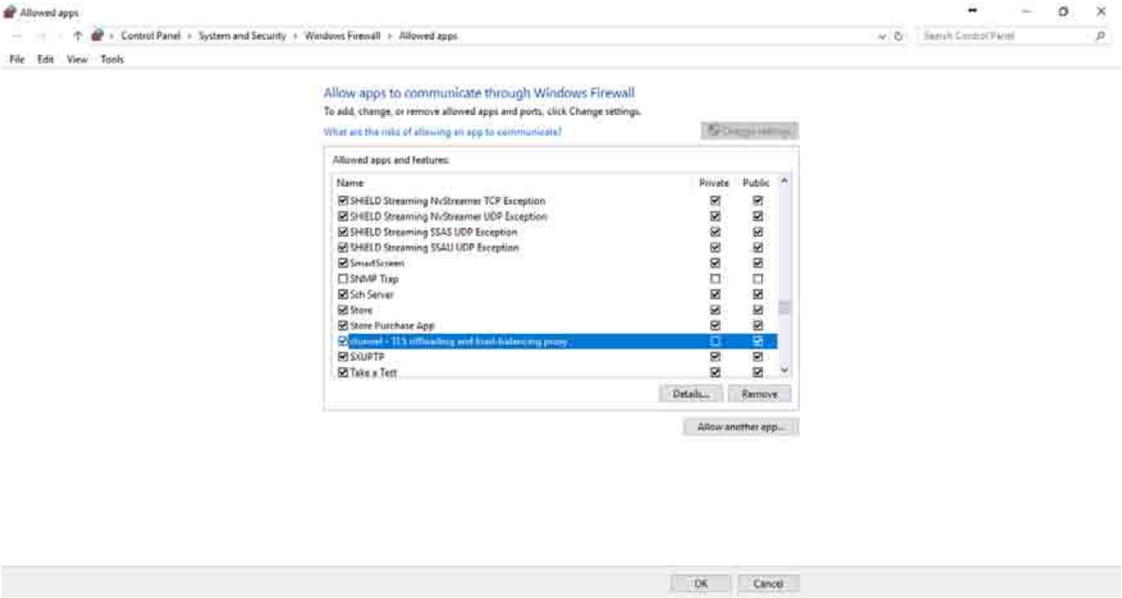
□ Enable multicasting of live streams from servers to clients.

IP Address

Port

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

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



Allow apps to communicate through Windows Firewall

To add, change, or remove allowed apps and ports, click Change settings.

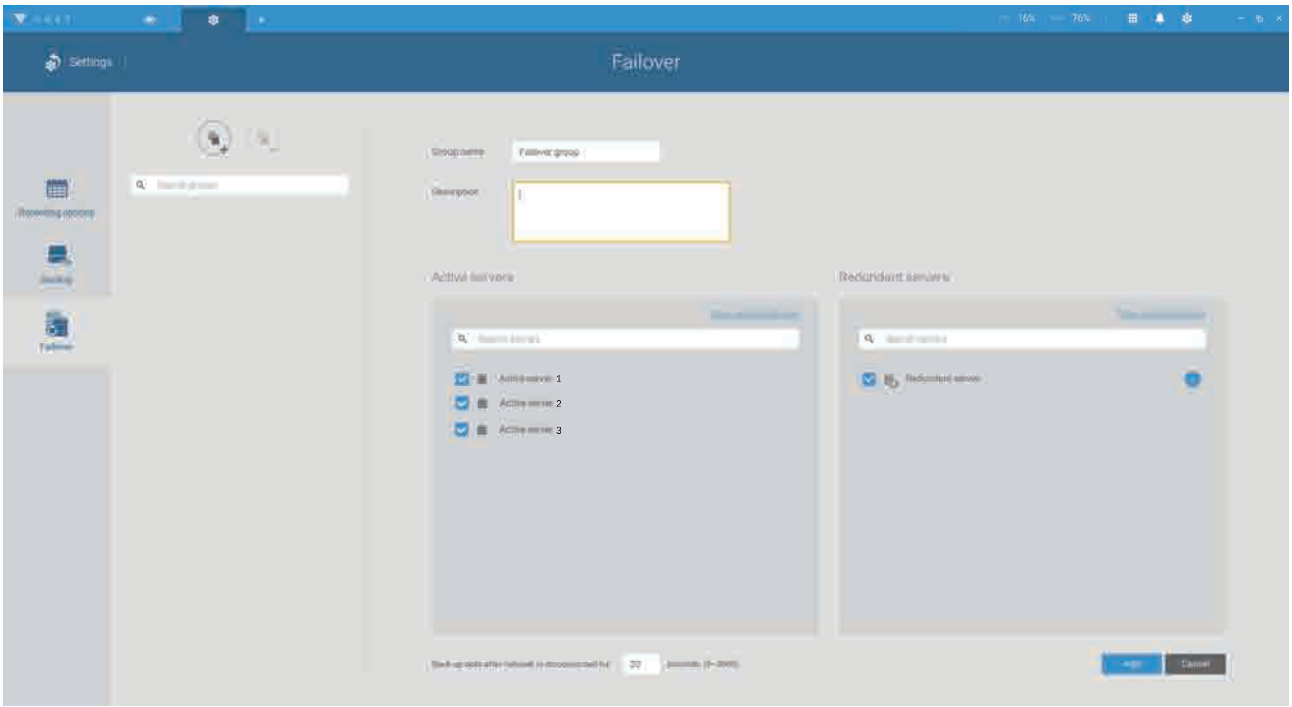
What are the risks of allowing an app to communicate?

Allowed apps and features:

Name	Private	Public
☑ SHIELD Streaming NvStreamer TCP Exception	☑	☑
☑ SHIELD Streaming NvStreamer UDP Exception	☑	☑
☑ SHIELD Streaming SSAS UDP Exception	☑	☑
☑ SHIELD Streaming SSAU UDP Exception	☑	☑
☑ SmartScreen	☑	☑
□ SNMP Trap	□	□
☑ Ssh Server	☑	☑
☑ Store	☑	☑
☑ Store Purchase App	☑	☑
☑ stunnel - TLS offloading and load-balancing proxy	□	☑
☑ SXUPTP	☑	☑
☑ Take a Test	☑	☑

Click on the Add button to create a Redundant server group. The Active and Redundant servers you enlisted on the Stations 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.



Group name: Failover group

Description:

Active servers

☑ Active server 1
☑ Active server 2
☑ Active server 3

Redundant servers

☑ Redundant server

Back up data after network is disconnected for 30 seconds (5~3600)

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.

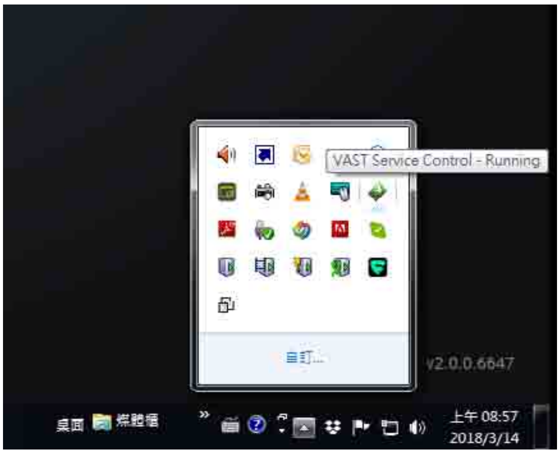
Note that the configuration of detection methods in People Counting still occur on a web console to individual cameras. It is not configurable through the VAST LiveClient.

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.

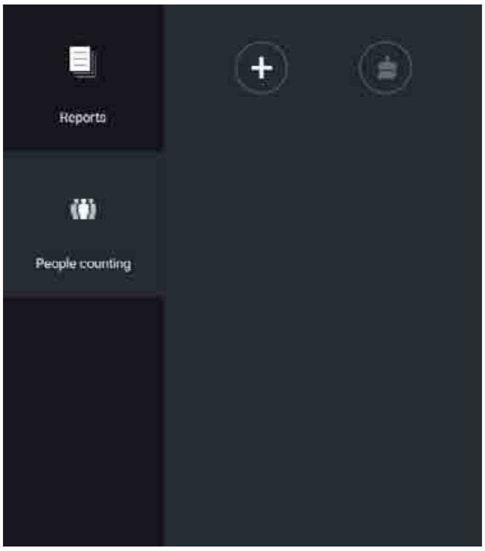
3. The life expectancy of VCA records is 5 years.

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

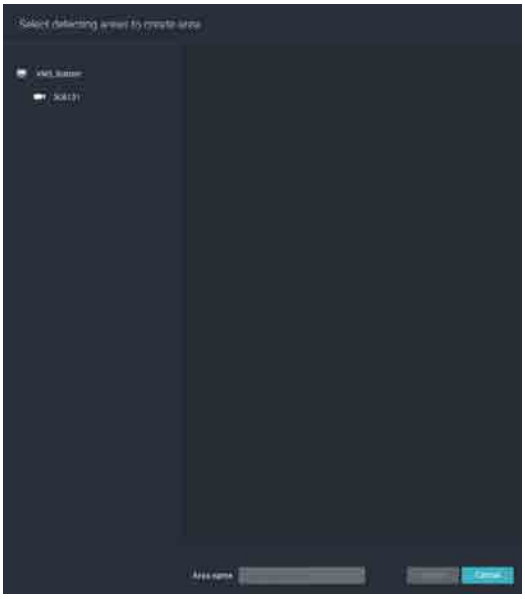
5. The latest revision VAST supports Seamless Recording, in order to retrieve collected data and recording during Ethernet disconnection. Provided that an SD card is installed on the VCA-enabled cameras, the VAST station gradually retrieves data from the SD card after the connection is restored.

To start VCA report:

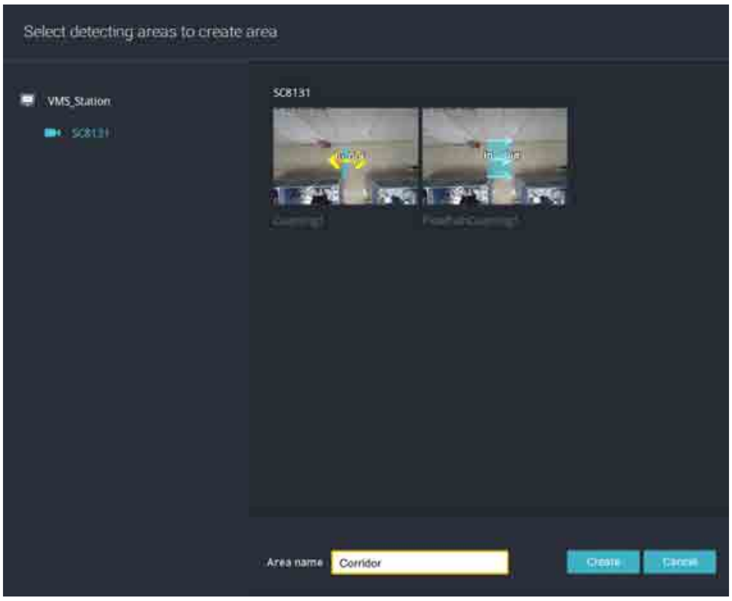
1. Click on VCA report button on the tool bar.
2. Select People Counting.
3. Click on the Add area ⊕ button.



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.

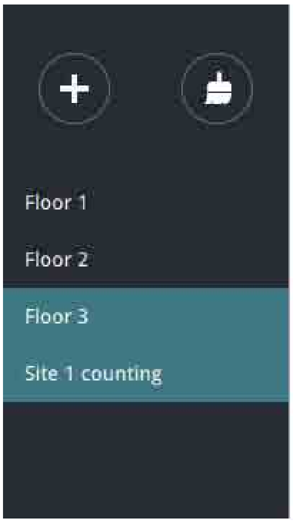


Select detecting areas to create area

Area name: Corridor

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.

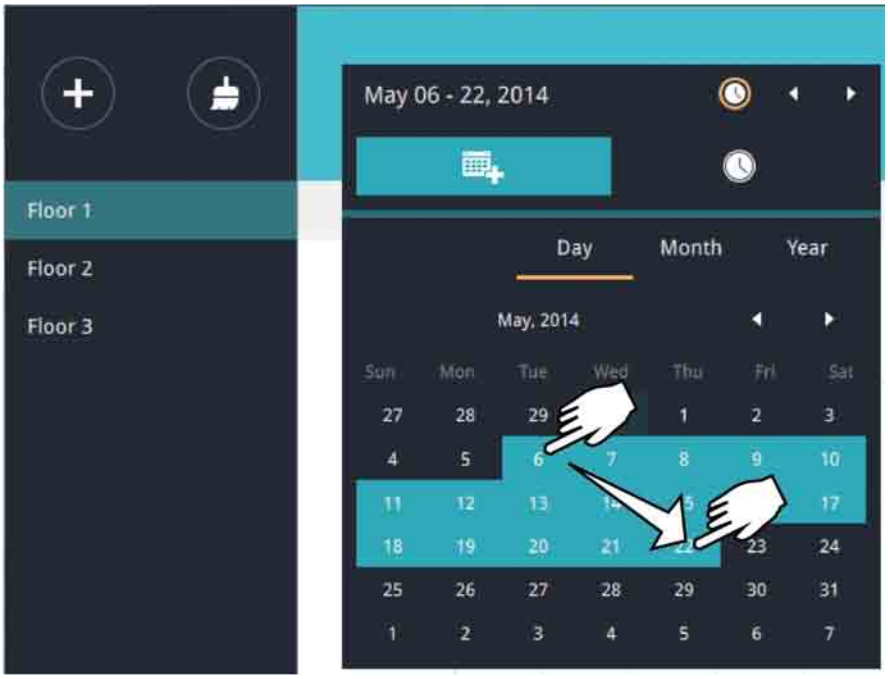


7. Select Date & Time

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.

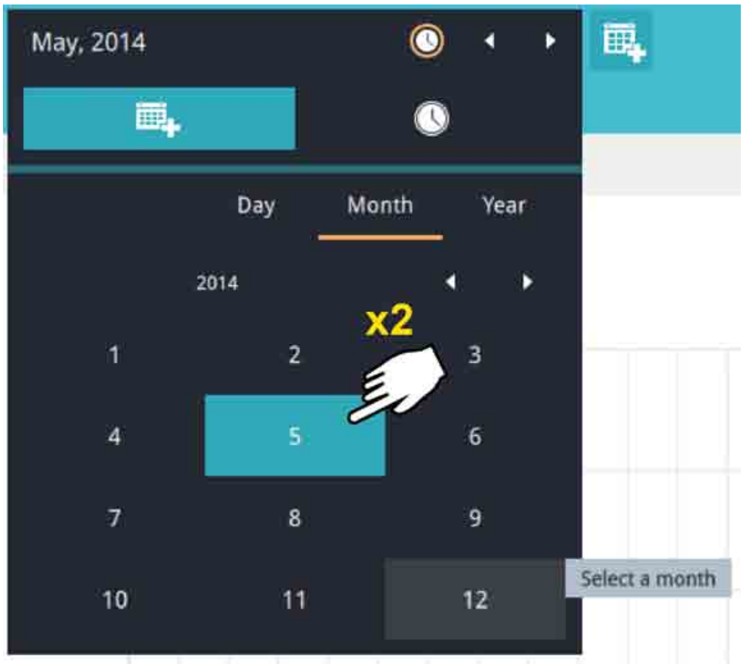
> Single-click to select a date or click and drag to select multiple dates.
> You can select a month or a year using a single click. If you select a month, the timeline unit will be days within the month. If you select a year, the timeline units will be the months in a year.
> In the **Month** or **Year** 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.



Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29		1	2	3
4	5	6	7	8	9	10
11	12	13	14	15		17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

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

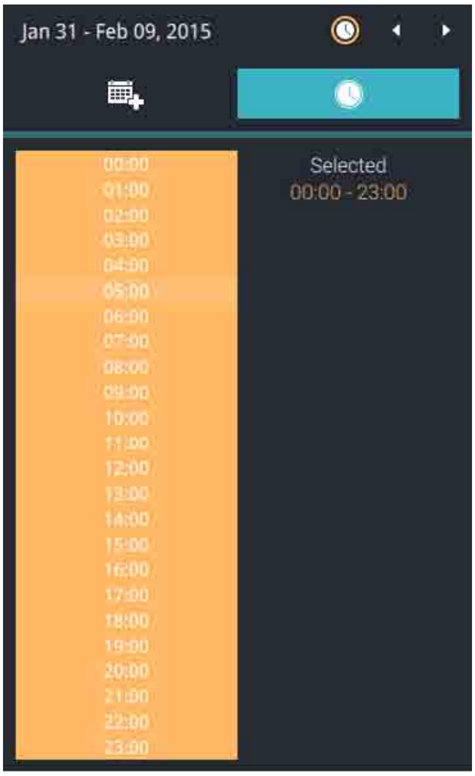
On a **Month** panel, double-click to select a month, and the **Day** panel for that particular month will display.



Note the following when making the configuration:

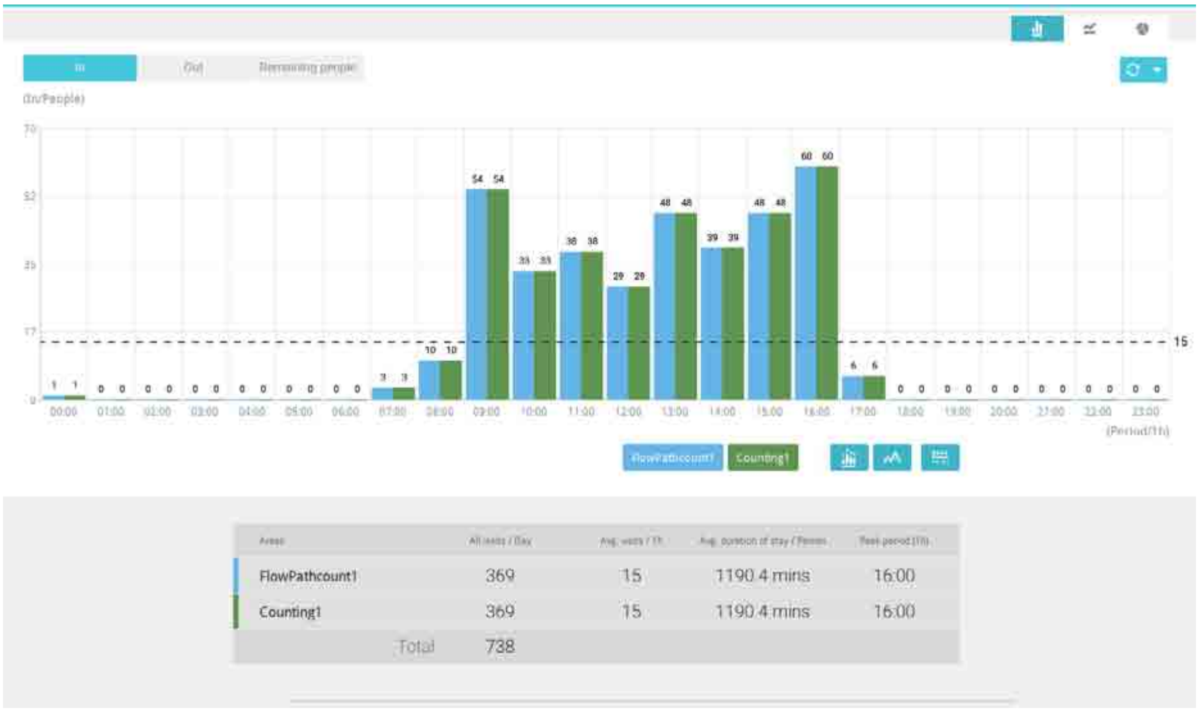
- When a date is selected, the Date and Time panel will not automatically close, and the configuration changes will not take effect until it is closed. You can click on the outside of the panel to leave the panel.
- You can select multiple days to form a span of time. Select one date with a single click and select multiple dates by draging your cursor across the screen to an end date you prefer.
- 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.



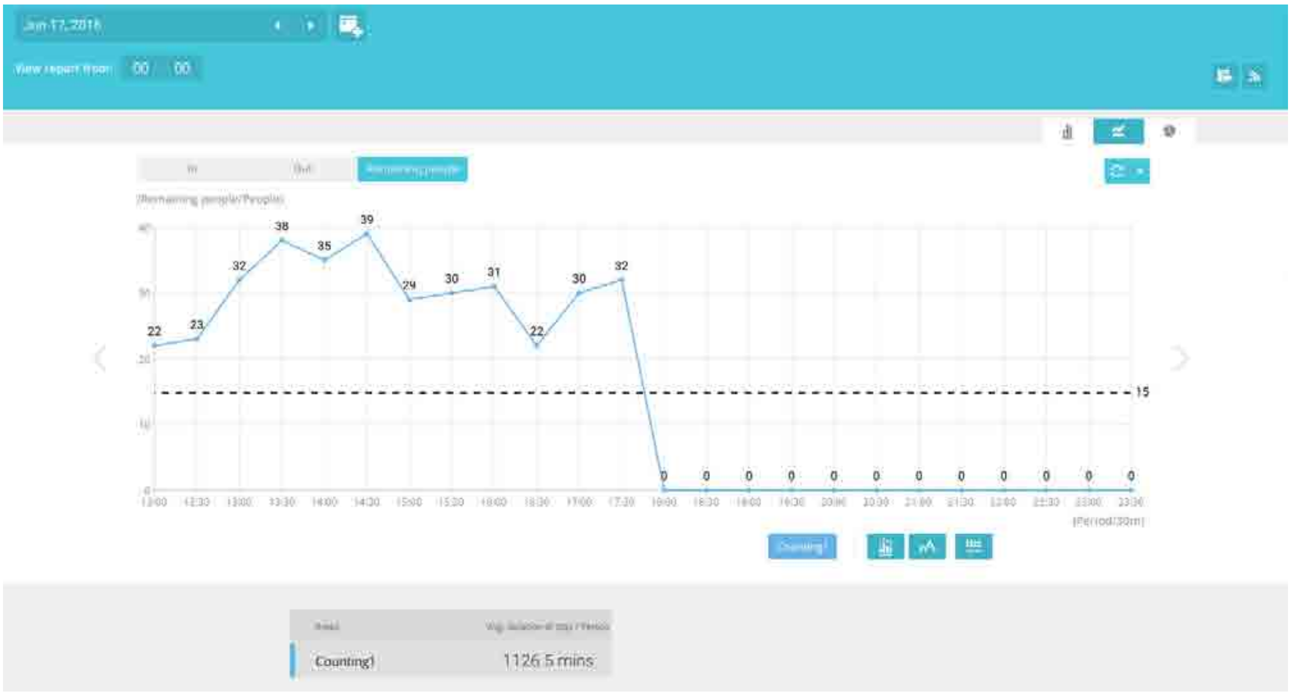
Note that you can only compare the counting results from two spans of time if you select only one Area. If you selected multiple Areas, you can not compare the results from multiple time spans.

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

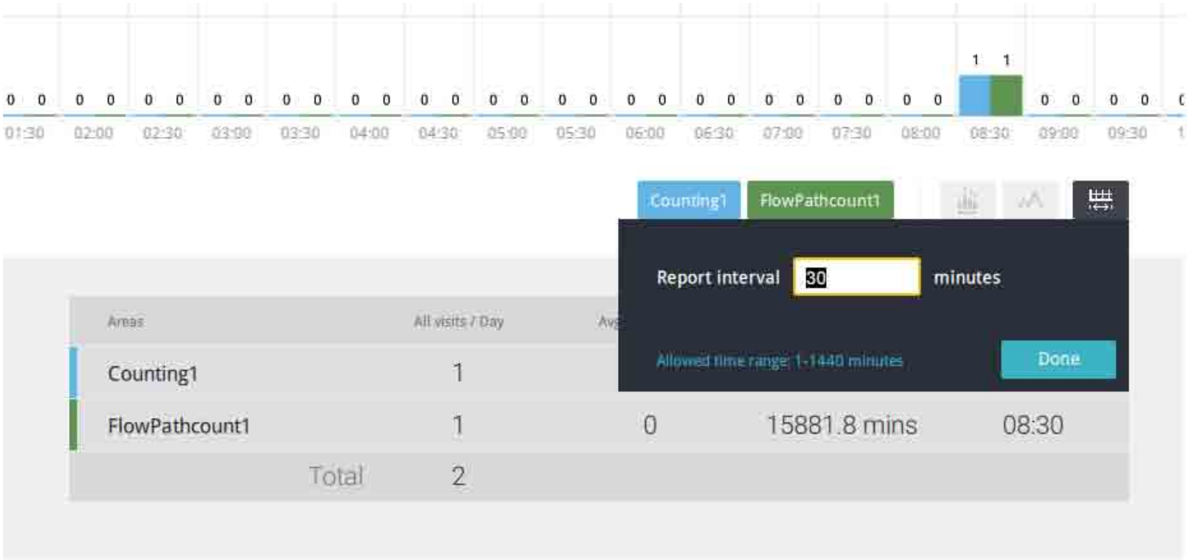
Note that the timeline units can vary depending on the span of time you selected on the Calendar panel. If a date was selected, hourly data will display in chart. If a year was selected, monthly data will display in chart.

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.



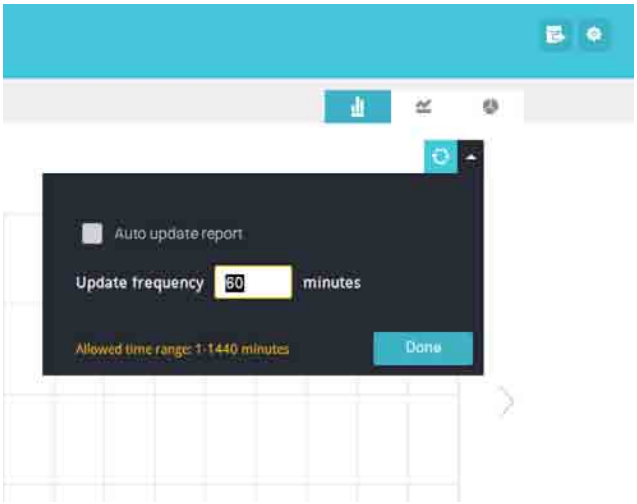
Report interval 30 minutes

Allowed time range: 1-1440 minutes

Done

Areas	All visits / Day	Avg		
Counting1	1			
FlowPathcount1	1	0	15881.8 mins	08:30
Total	2			

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.



□ Auto update report

Update frequency 60 minutes

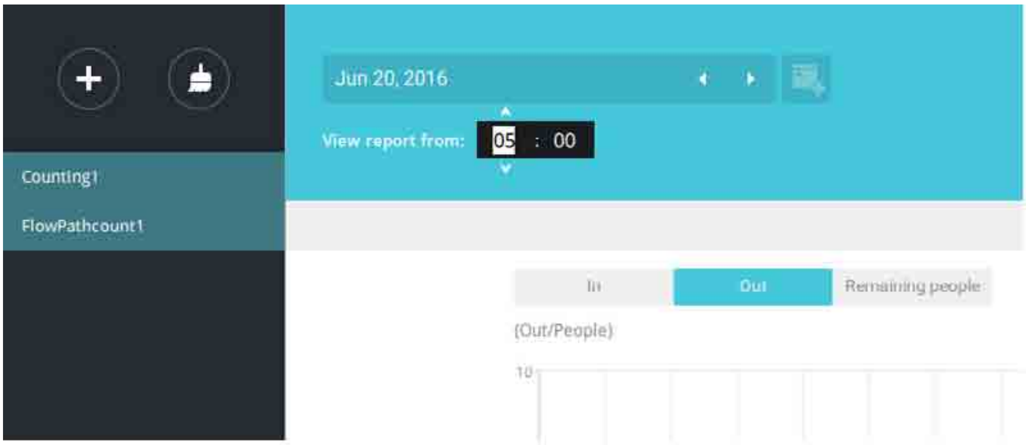
Allowed time range: 1-1440 minutes

Done

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.

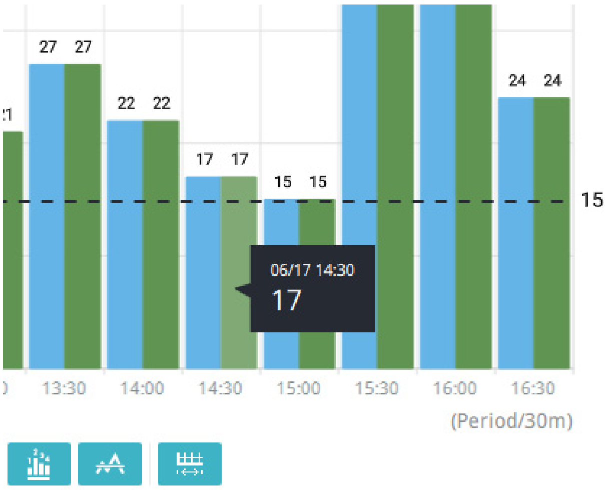
Use the **Refresh** button ↻ to poll the latest data from camera.

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.


Jun 20, 2016

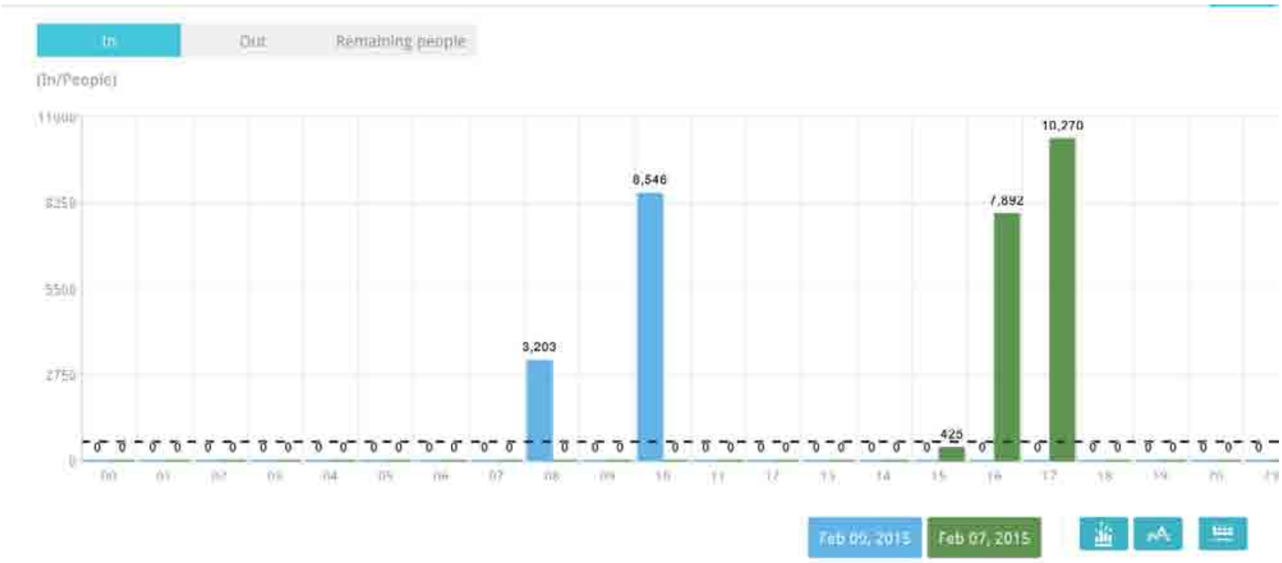
View report from: 05 : 00

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.

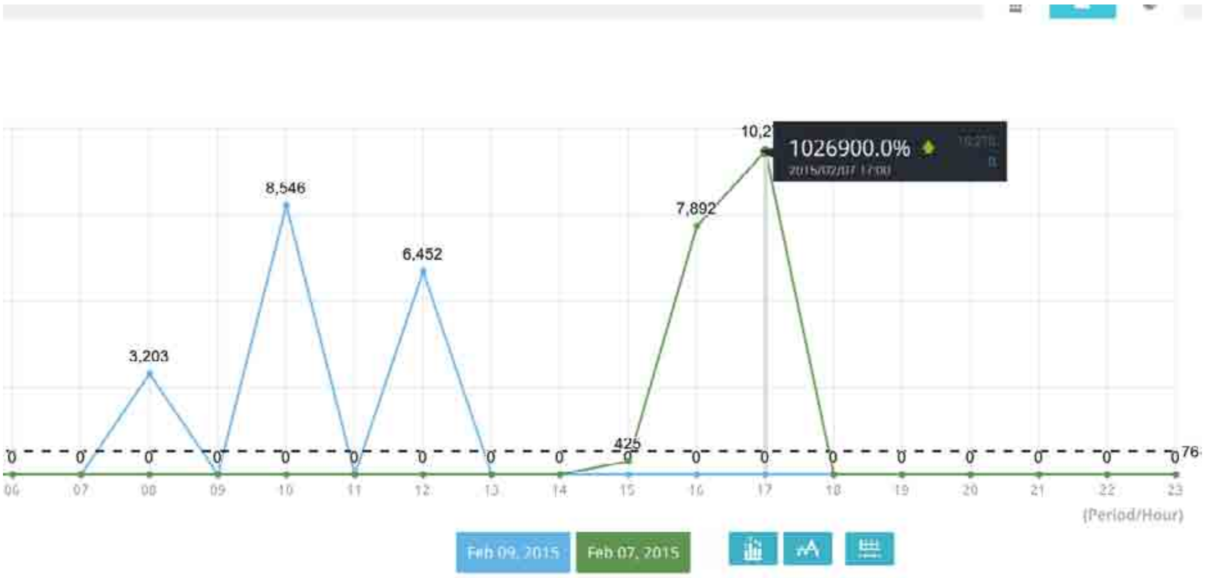


Data on a time line will be generated. To close the window, use the close button on the second date information. Equivalent spans of time can also be used for comparison. For example, you can compare the data in a span of 4 days against another span of 4 days.

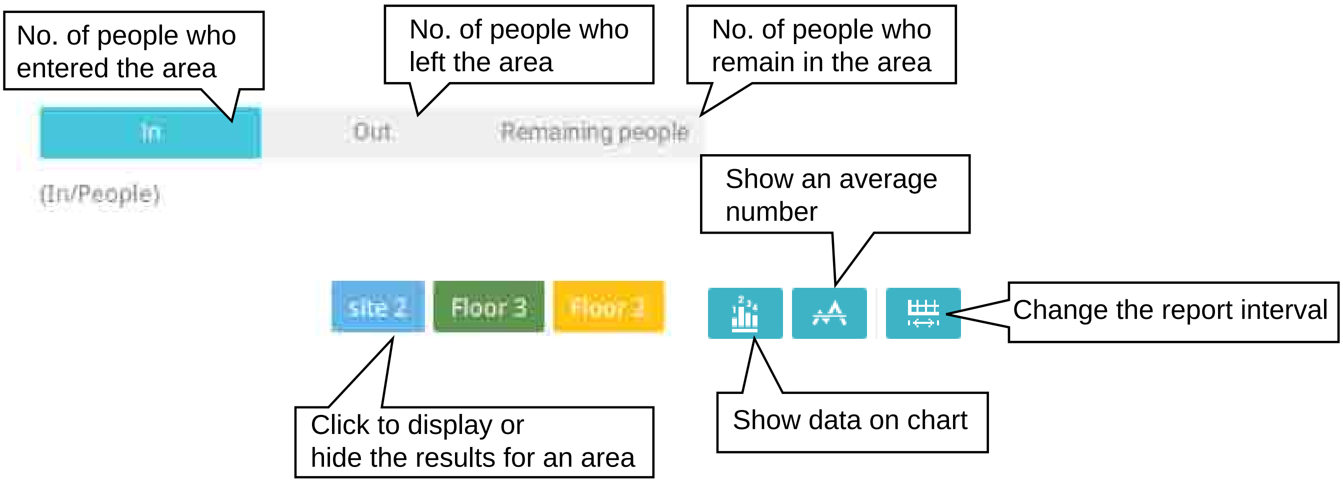
Note that the **Compare** function only applies when you select to display only one area on the screen.



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.



No. of people who entered the area

No. of people who left the area

No. of people who remain in the area

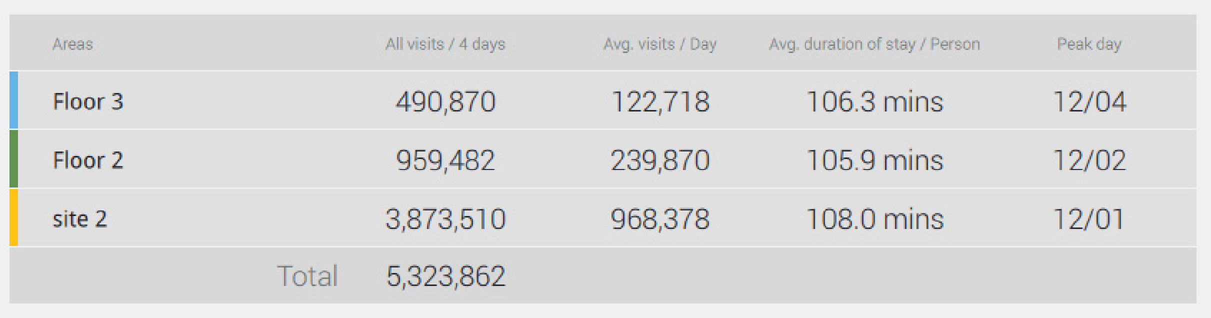
Show an average number

Change the report interval

Click to display or hide the results for an area

Show data on chart

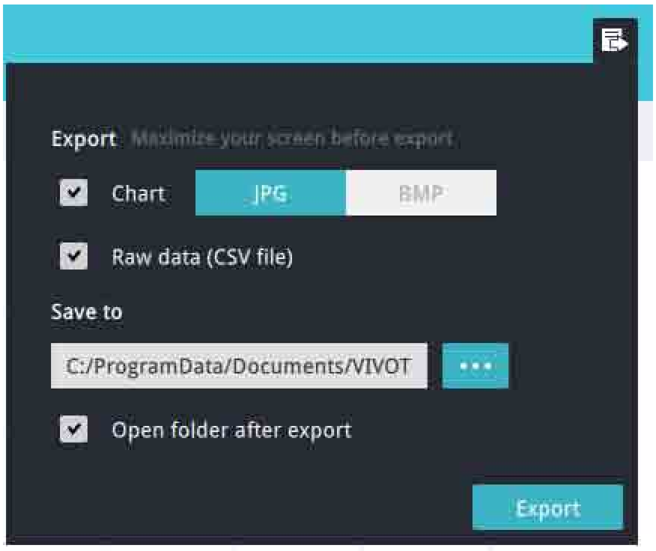
In addition to the charts, a summary of displayed data will be listed below showing the areas involved, visits/Day or Month, Average visits / Hours / Days, Average duration of stay / person, and the Peak hour.



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



Export Maximize your screen before export

☑ Chart JPG BMP

☑ Raw data (CSV file)

Save to

C:/ProgramData/Documents/VIVOT ...

☑ Open folder after export

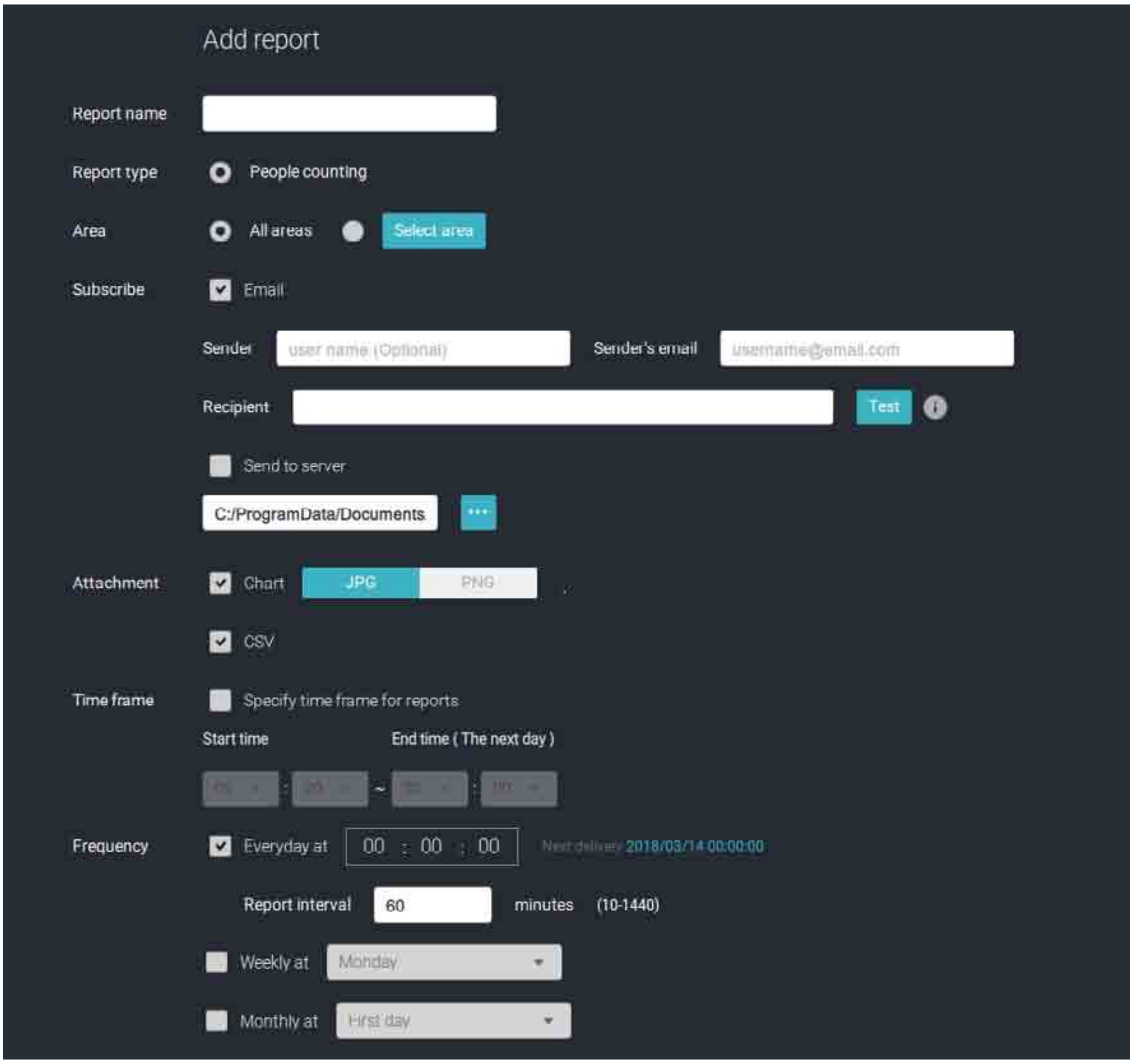
Export

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 the 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.



Add report

Report name

Report type ● People counting

Area ● All areas ○ Select area

Subscribe ☑ Email

Sender user name (Optional) Sender's email username@email.com

Recipient

□ Send to server

C:/ProgramData/Documents

Attachment ☑ Chart JPG PNG

☑ CSV

Time frame □ Specify time frame for reports

Start time End time (The next day)

Frequency ☑ Everyday at 00 : 00 : 00 Next delivery 2018/03/14 00:00:00

Report interval 60 minutes (10-1440)

□ Weekly at Monday

□ Monthly at First day

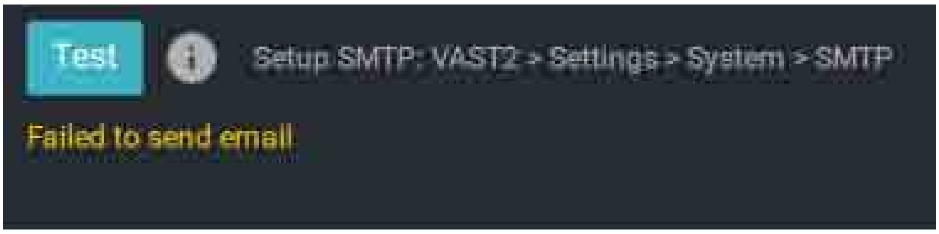
Note that the notification contents is your current field of view, including a Bar, Line, and Pie chart combined into one image file. The In/Out/Remaining results will be generated into 3 charts. Each Area will generate one CSV file, and each CSV data file will contain In/Out/Remaining/Summary information.

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 an 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.



Setup SMTP: VAST2 > Settings > System > SMTP

Failed to send email

3-4. VAST Software License

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

User	Scenario	Action
Software license users MAC license users	New users need to use VAST w/o a purchased license	1. Purchase license and get license key from sales representative or distributor. 2. Go to Settings > System > License > Activate official version > Online activation > Activate complimentary license. 3. Select stations and activate license.
Software license users	New or current users need to use VAST with a purchased license	1. Purchase license and get license key from sales representative or distributor. 2. Go to Settings > System > License > Activate official versin or Update Official license > Online activation > Activate with license key. 3. Select stations and input license key to activate license.
MAC license users Dongle license users	New or current users to use VAST with a purchased license	1. Go to Settings > System > License > Activate official version > Offline activation > Export request file 2. Send license request file (.req) to sales representative or distributor to purchase more dongle license 3. Go to Settings > System > License > Activate official version > Offline activation > Import license file (Dongle users) or Import MAC license (MAC users)

Revision 2.12:
Trial versioin or Free standard version:
If Free standard version is selected, 32 free channels will be available. If Trial version is selected, a 256 channel license is free to use for 60 days.

Revision 2.13:
The above trial and free options will not be available for revision 2.13 or later.

When VAST is installed, it is in a state of unliccensed condition. Users need to activate the licenses as the official version or trial version via the online or offline methods.

If upgrading from rev. 2.12 or earlier to rev. 2.13, the original free channels will need to be activated using the new activation process. With the purchased channels, you do not need to re-activate them.

Unlicensed: Without activation or insufficient number of licenses.
In this state, VAST client will be logged out every 60 minutes. The camera live view, playback, and recording services will stop in 14 days. Users will need to activate or purchase the licenses after 14 days.

Official version: Activated via the Complimentary license or the purchased license key.

Complimentary license: When connected to VIVOTEK's authorization website, the complimentary licenses will be acquired with the number of the current VIVOTEK cameras and substations in use (not including ONVIF cameras). If users install more cameras or substations later, the complimentary licenses should be activated once again. The maximum number of the complimentary licenses will be updated and published on the https://www.vivotek.com/vast2#license. Currently 32 channels is available, but the number is subject to change.

License key: For official camera licenses or advanced licenses.
Contact your sales representatives or distributor to purchase licenses. You will receive license keys and activate them through the online or offline activation.

For Online activation, VAST will upload the license request file (.req file) and license key to the license portal automatically. After the authorization process, you will receive the license file (.lic file).

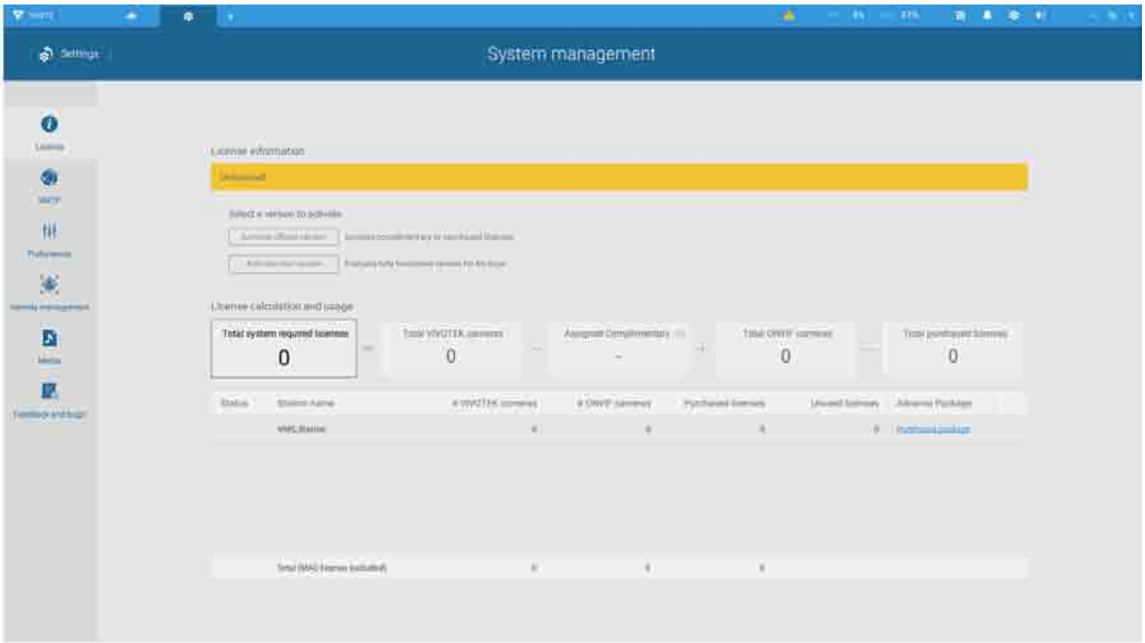
For Offline activation, users will need to handle the process manually on the license activation portal. Upload the license request file (.req file) and license key to the license portal. After the authorization process, you will receive the license file (.lic file).

NOTE:

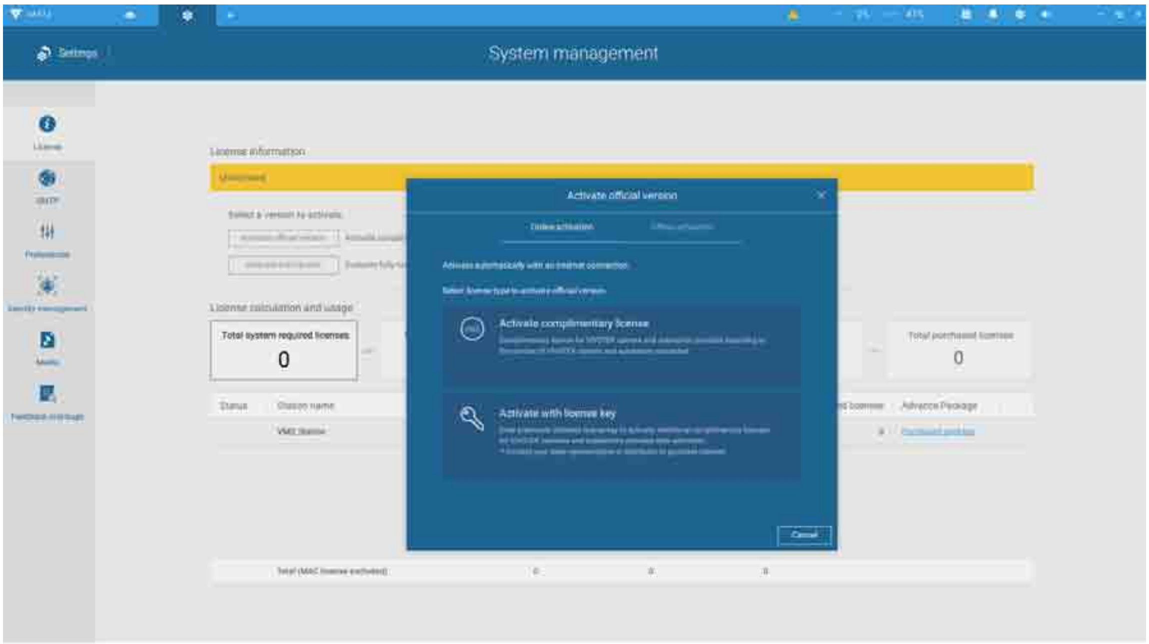
- The new activation process does not apply for users using hardware dongle license or licenses on virtual machines.
- Finish installing all of your cameras and substations before activating the complimentary licenses to avoid activating those added licenses again.
- Keep a copy of the license key for future reference.

Activation process:

Go to **Settings** > **System** > **License** page,
and select **Activate official version** or **Activate trial version.**



If the Activate official version is selected,

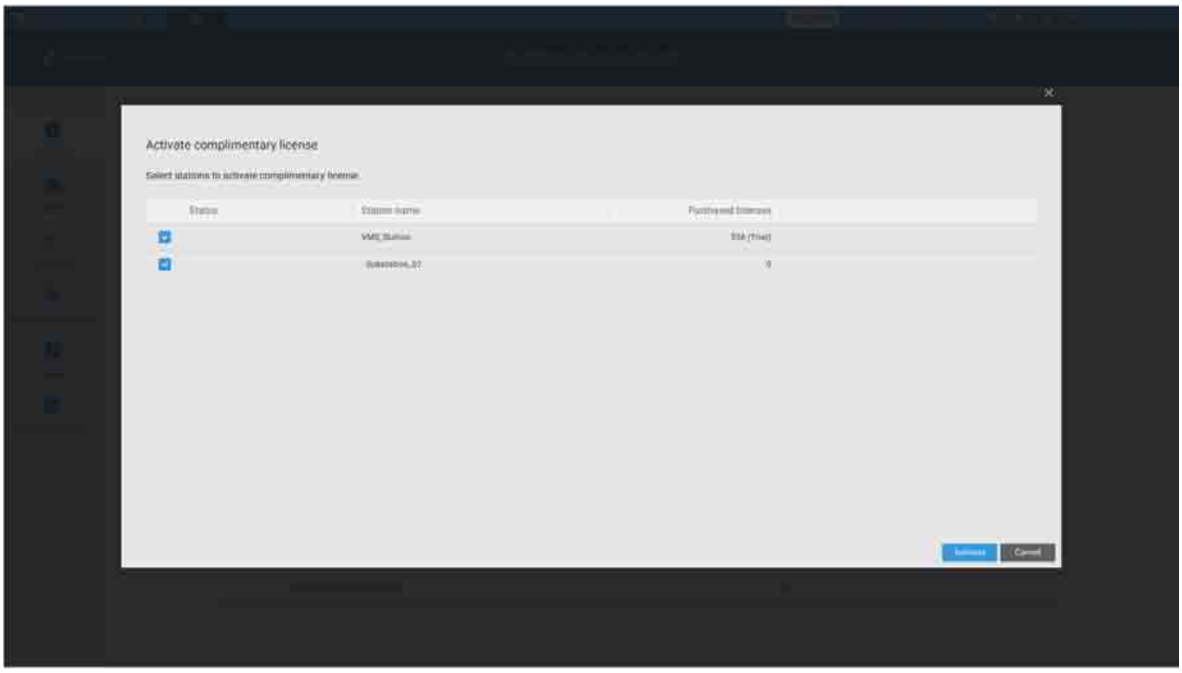


If you have Internet connection, select **Online activate**.

If not, select **Offline activate**.

If your VAST deployment does not require purchasing licenses, select **Activate complimentary license**. , If you have purchased license and acquired license key, select **Activate with license key**.

If you want to use the complimentary license, select to apply to the current station and substation, and then click **Activate**.

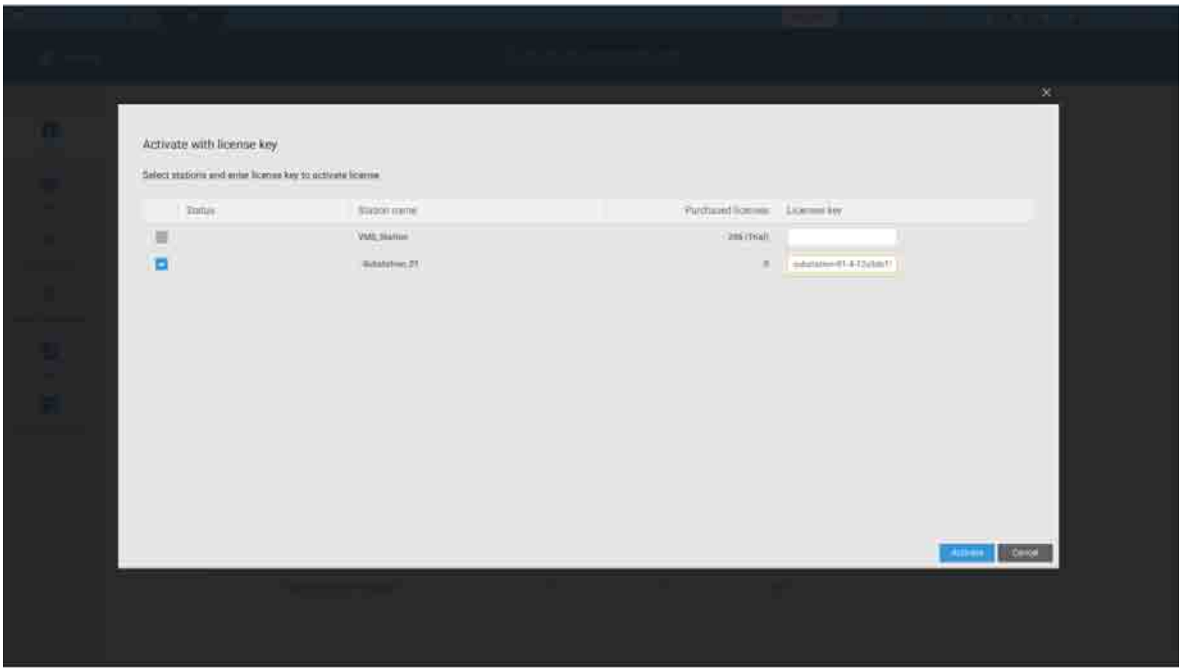


Activate complimentary license

Select stations to activate complimentary license

	Status	Station name	Purchased licenses
☑		VMS_Station	256 (Trial)
☑		Substation_01	0

If you select **Activate with license key**, slect the station where the license key will apply to. Enter the license key.

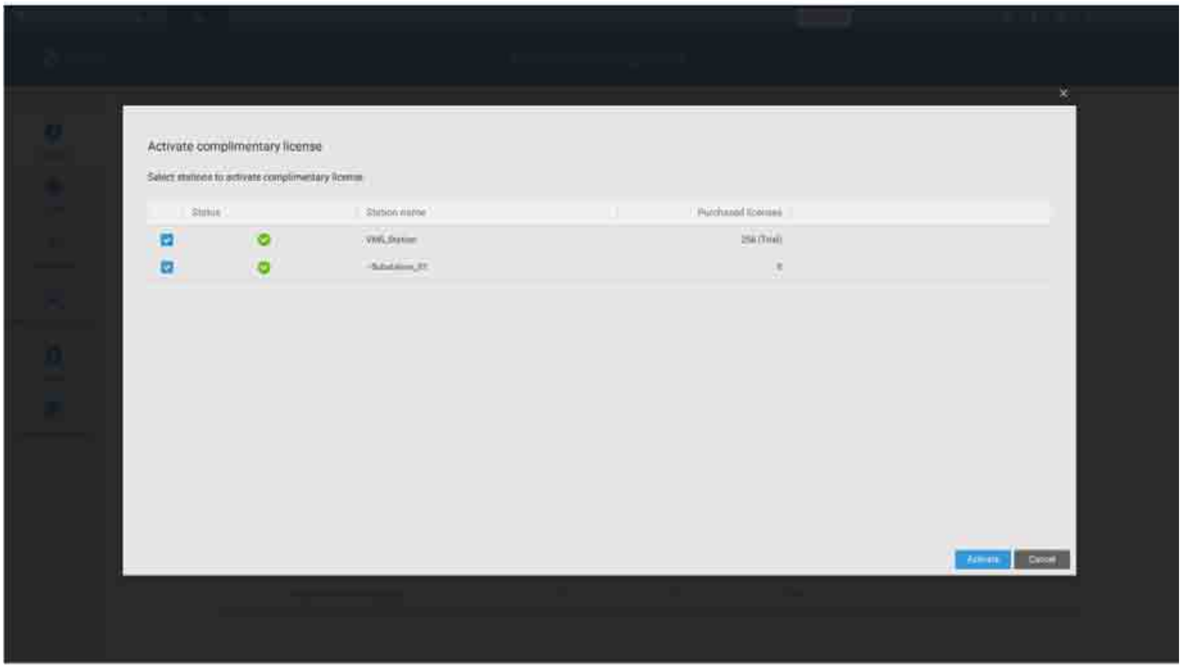


Activate with license key

Select stations and enter license key to activate license

	Status	Station name	Purchased licenses	License key
□		VMS_Station	256 (Trial)	
☑		Substation_01	0	substation-01-4-12a5de1

When successfully activated, the associated check circles will turn grren. Click the Close button on the upper right of the screen.

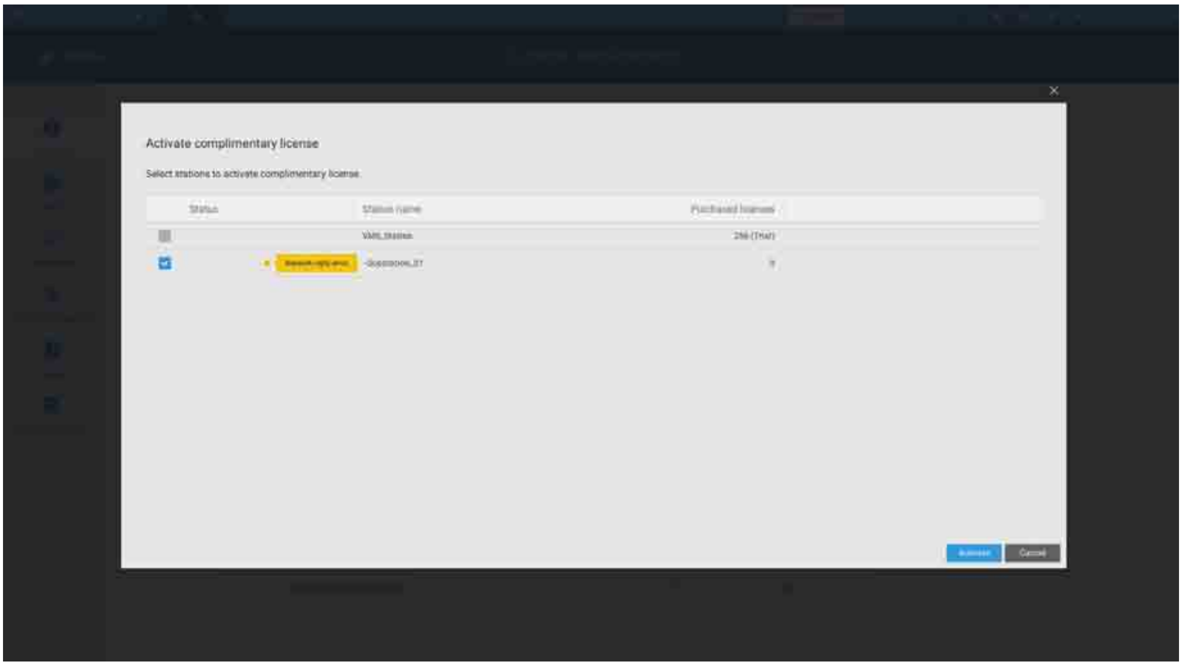


Activate complimentary license

Select stations to activate complimentary license

	Status	Station name	Purchased licenses
☑	✓	VMS_Station	256 (Trial)
☑	✓	-Substation_01	8

If you fail, status bar will turn yellow with an alarm icon, and the possible reason will be listed.

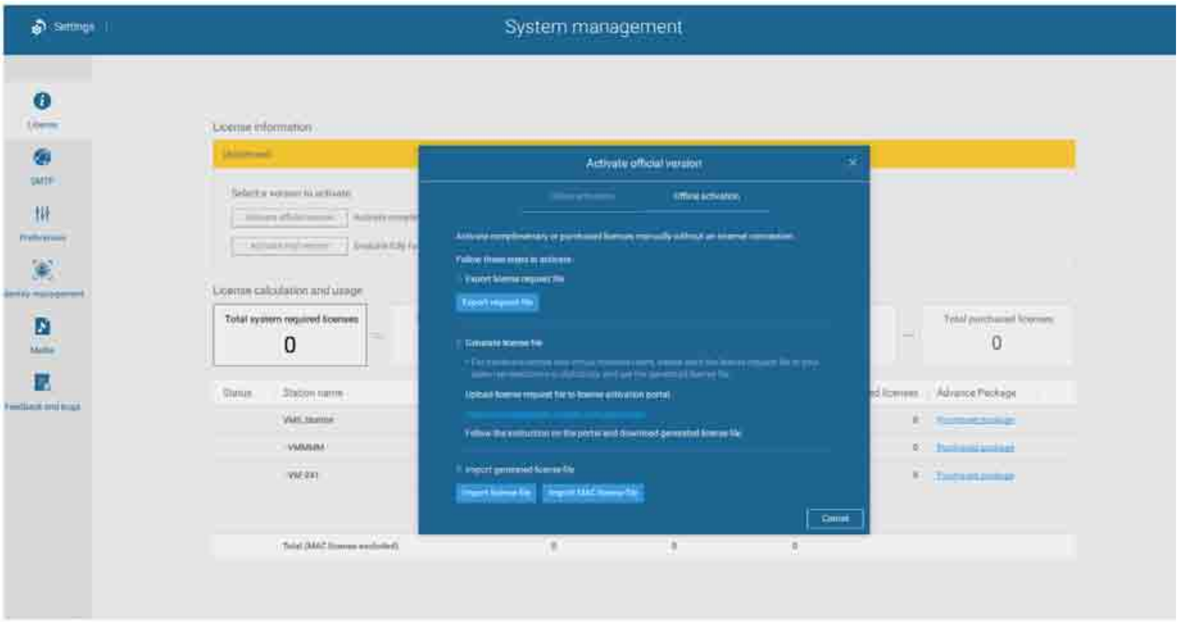


Activate complimentary license

Select stations to activate complimentary license

	Status	Station name	Purchased licenses
□		VMS_Station	256 (Trial)
☑	[illegible]	-Substation_01	8

If your VAST station has no Internet connetion, select the Offline Activation option.



Settings

System management

License information

Activate official version

Online activation

Offline activation

Activate complimentary or purchased licenses manually without an internet connection.

Follow these steps to activate:

1. Export license request file

Export request file

2. Generate license file

For purchased license and virtual license users, please send the license request file to your sales representative to obtain and get the generated license file.

Upload license request file to license activation portal

Follow the instruction on the portal and download generated license file

3. Import generated license file

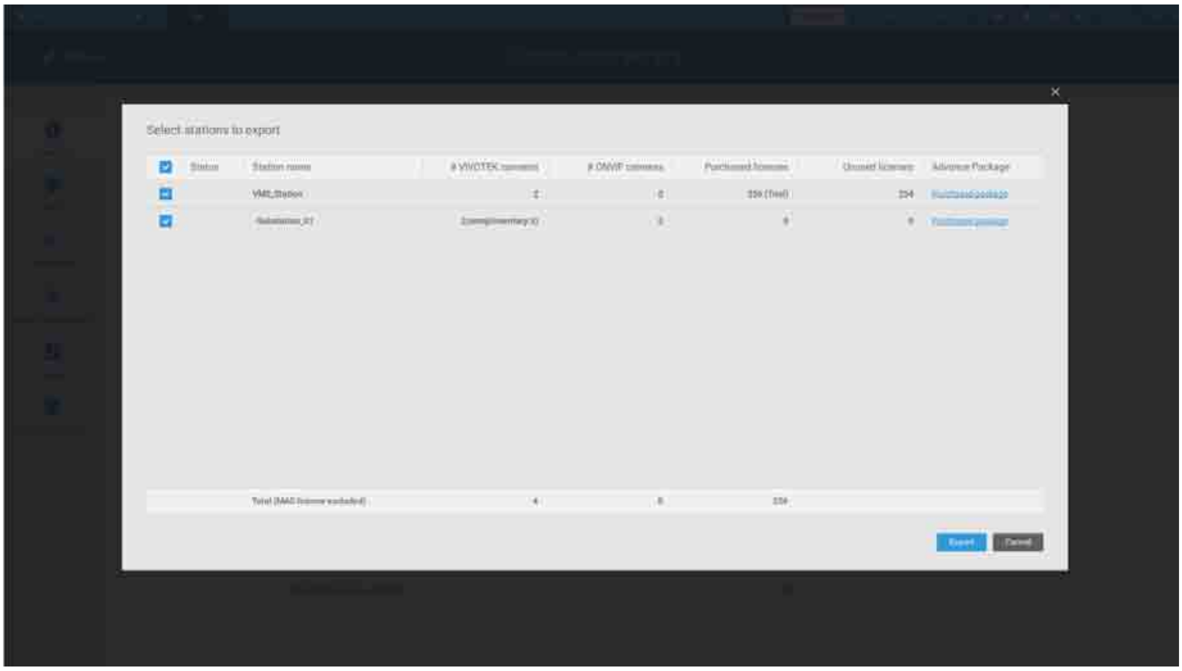
Import license file

Import MAC license file

Cancel

According to the instructions on screen,

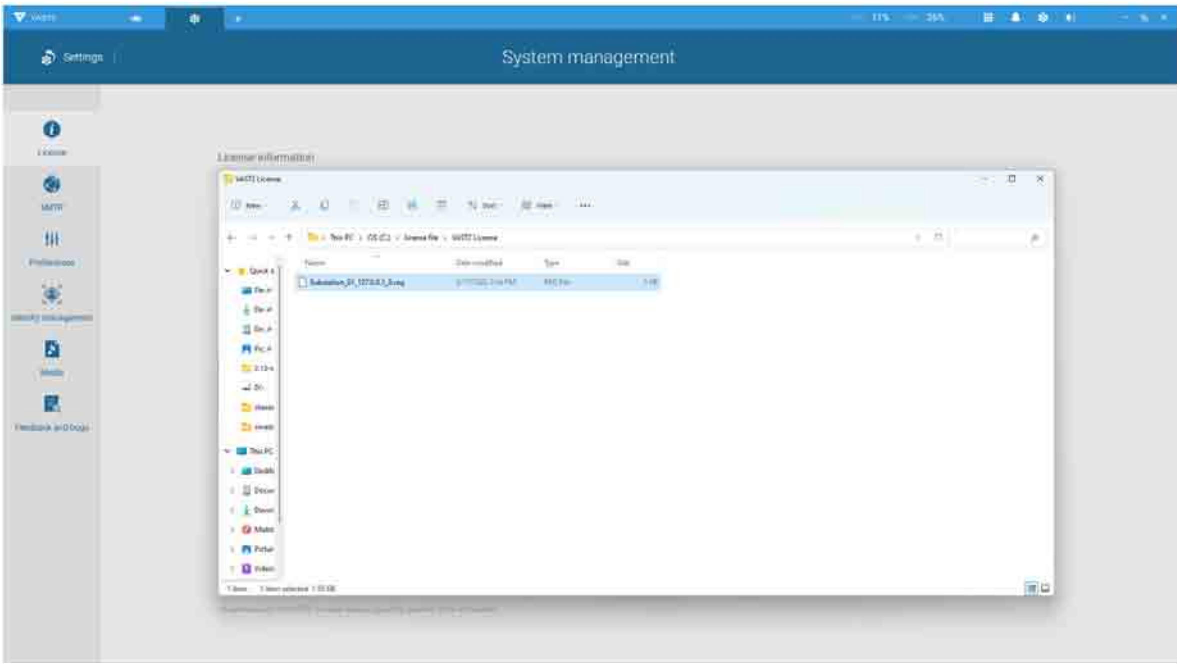
1. Export licensse request file.
2. Select the station to export the license request, click Export, and select the destination of the request file.



Select stations to export

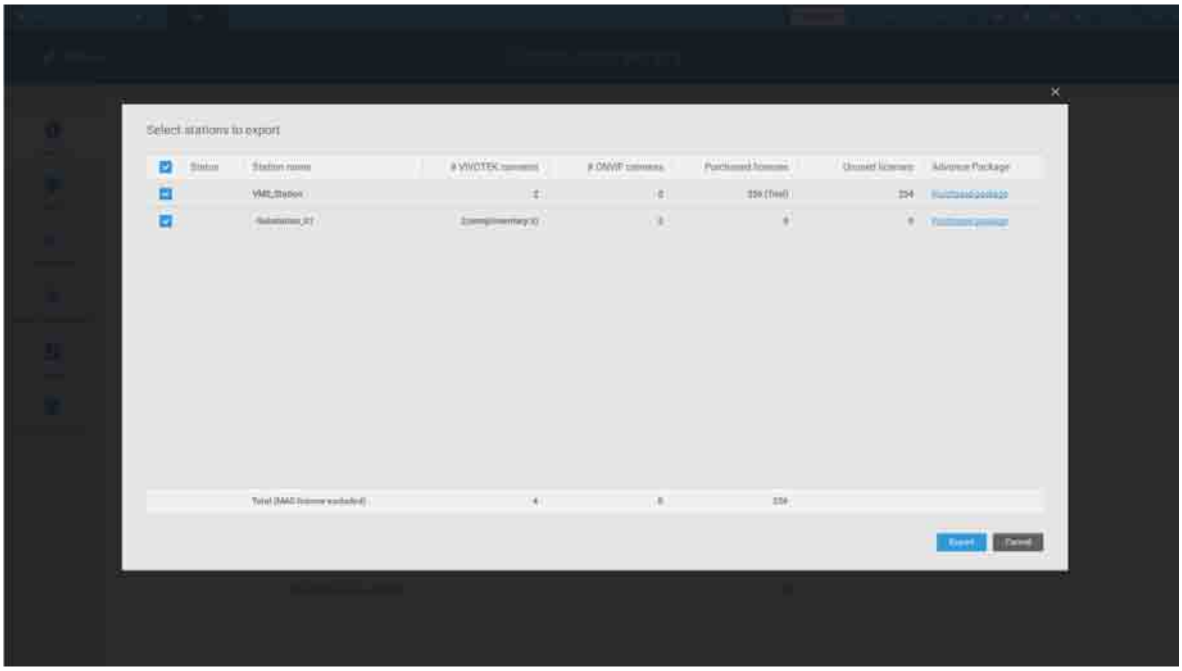
☑	Status	Station name	# VIVOTEK cameras	# ONVIF cameras	Purchased licenses	Unused licenses	Advance Package
☑		VMS_Station	2	0	336 (Trial)	334	Purchased package
☑		-Substation_01	2(complimentary:2)	0	0	0	Purchase package
		Total (MAC license excluded)	4	0	336		

The REQ file looks like the following.



3. Find a computer to upload the REQ file to VIVOTEK's license activation portal.

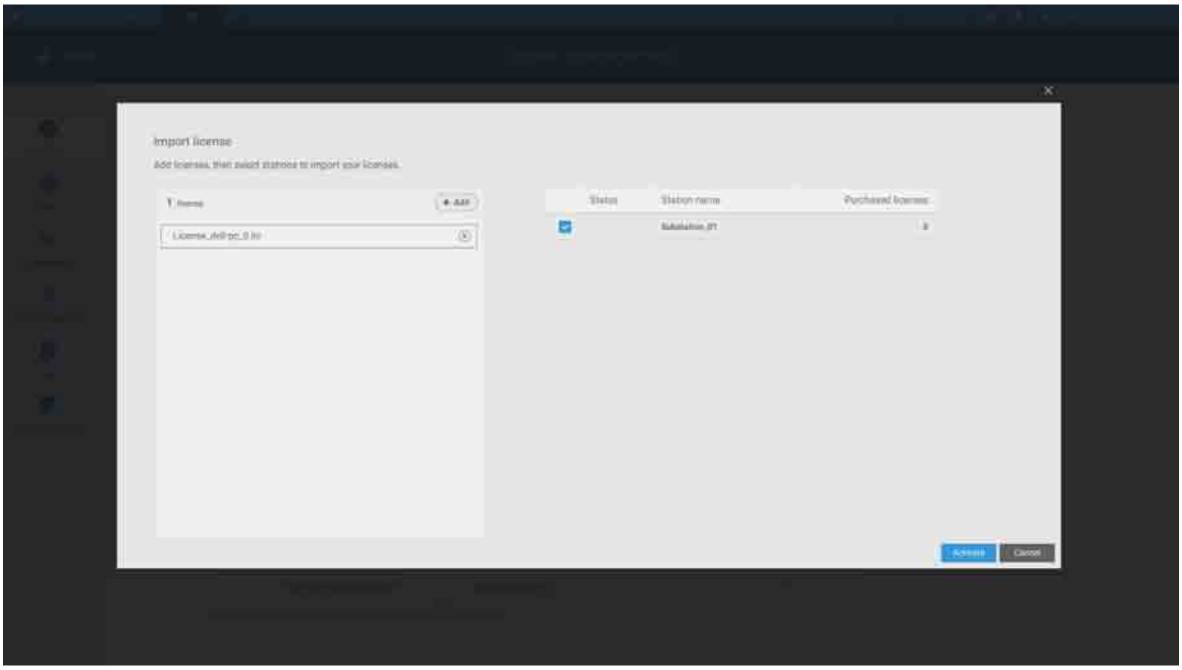
4. Follow the instructions on the license activation portal to download the license file (.LIC file). Upload or copy the file to your VAST station.



Select stations to export

☑	Status	Station name	# VIVOTEK cameras	# ONVIF cameras	Purchased licenses	Unused licenses	Advance Package
☑		VMS_Station	2	0	336 (Trial)	334	Purchase package
☑		Substation_01	2(complimentary:2)	0	0	0	Purchase package
		Total (MAS license excluded)	4	0	336		

5. On your VAST station, select import license file, click Add to select the license file (.LIC file), and click Activate.



Import license

Add licenses, then select stations to import your licenses.

1 Items

License_[illegible].lic

	Status	Station name	Purchased license
☑		[illegible]	[illegible]

Updating Licenses for VAST on Virtual Machines

NOTE:

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

This instruction includes:

1.How to Export a license request from VAST2 on a virtual machine.

2.How to acquire the MAC addresses of the inserted or non-inserted cameras?

3.Send us request files & MAC addresses (If you have multiple Stations, please remember to designate grouping information, such as which MAC addresses belong to which camera deployments).

4.How to Import MAC licenses to VAST2?

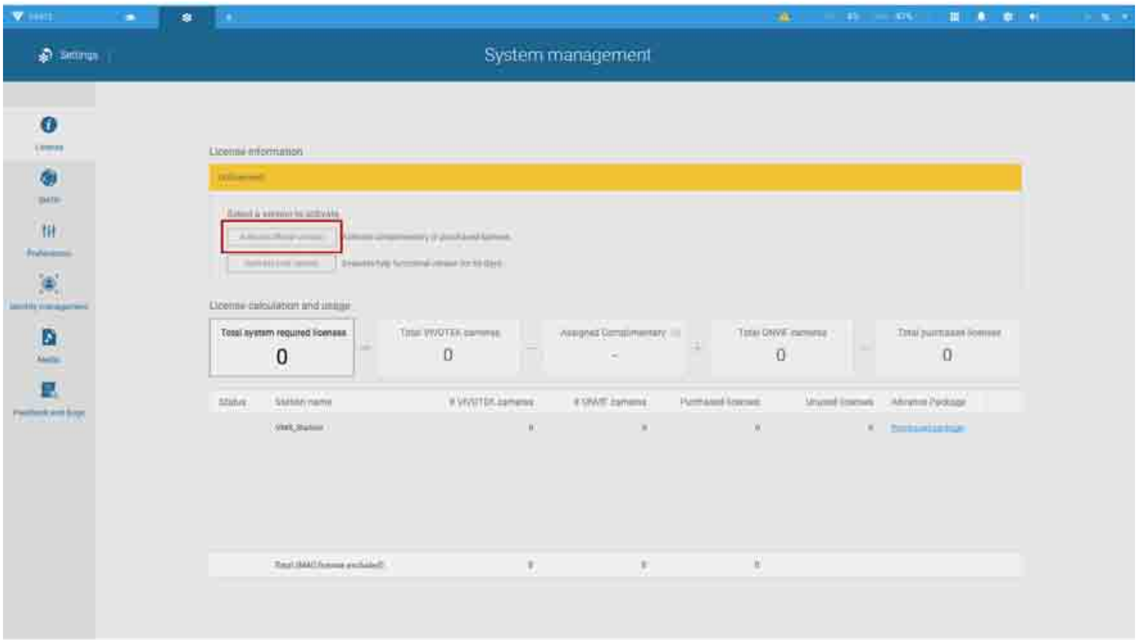
5.How to buy more MAC licenses for future distribution?

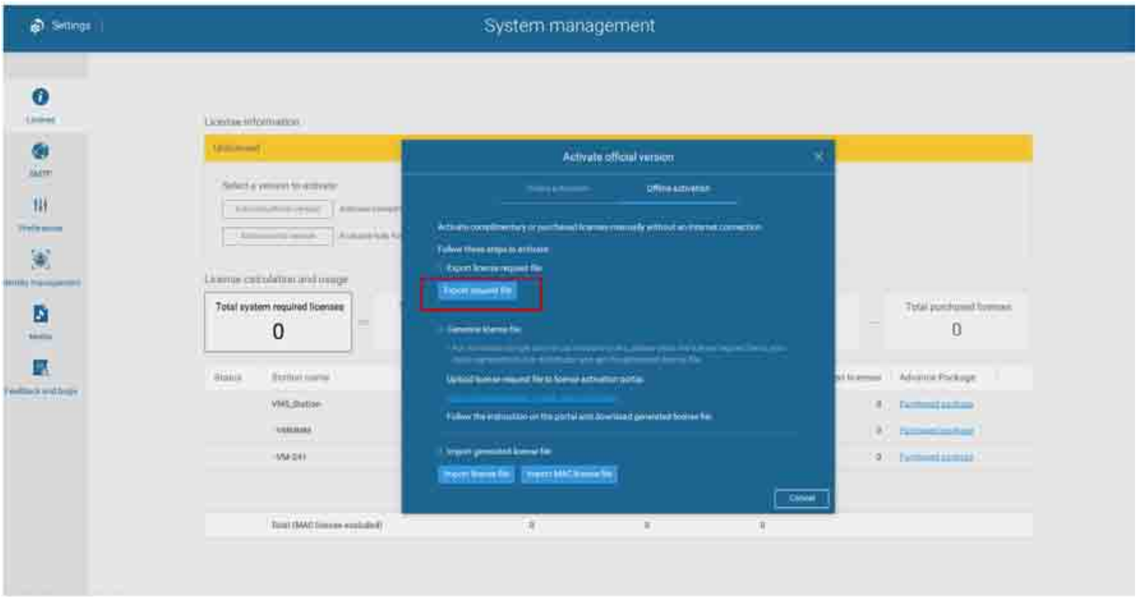
1.How to export request from VAST2 on VM?

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).
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.





Activate complimentary or purchased licenses manually without an internet connection.

Follow these steps to activate:

Export license request file

Generate license file

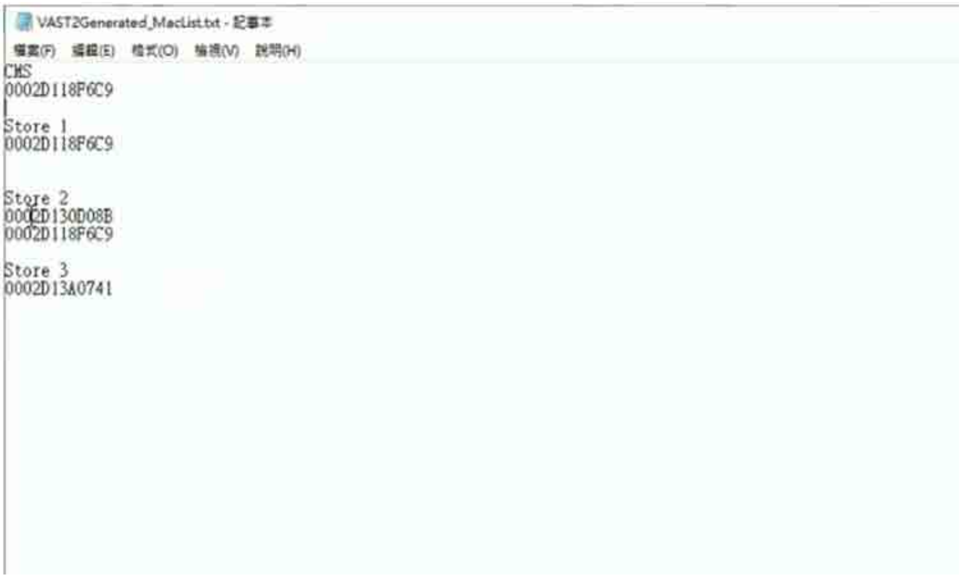
Upload license request file to license activation portal.

Follow the instruction on the portal and download generated license file.

Import generated license file

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.



VAST2Generated_MacList.txt - 記事本
檔案(F) 編輯(E) 格式(O) 檢視(V) 說明(H)

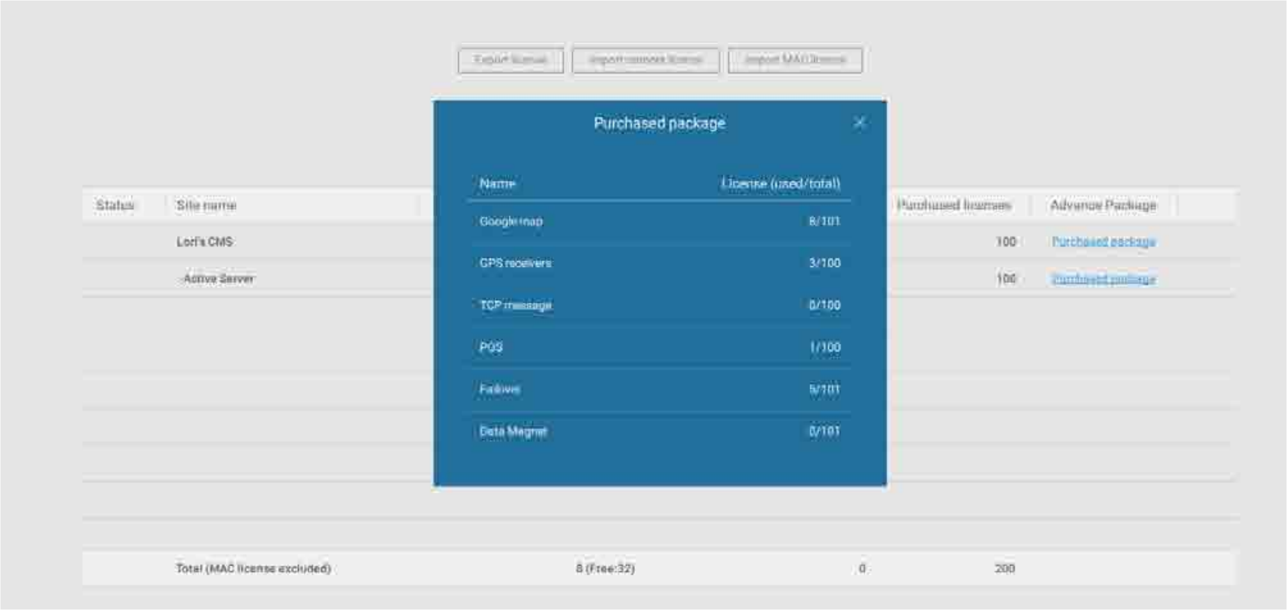
```
CMS
0002D118F6C9

Store 1
0002D118F6C9


Store 2
0002D130D08B
0002D118F6C9

Store 3
0002D13A0741
```

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



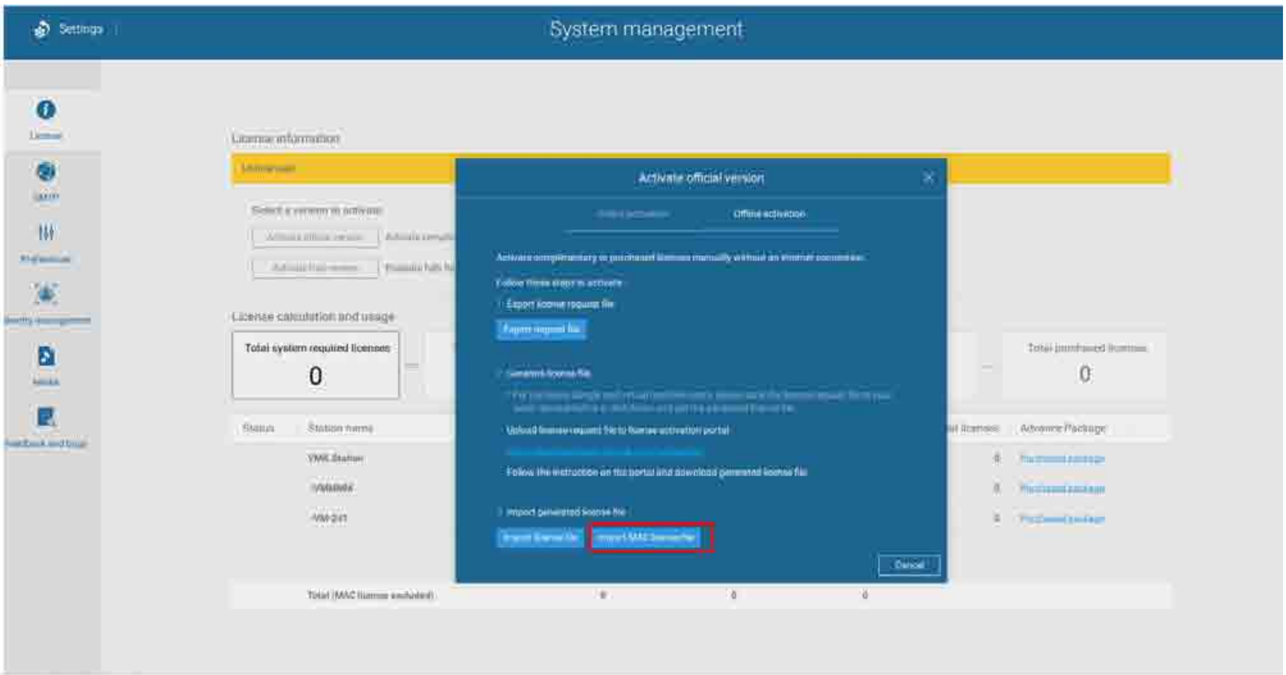
Purchased package

Name	License (used/total)
Google map	8/101
GPS receivers	3/100
TCP message	0/100
POS	1/100
Failover	5/101
Data Magnet	0/101

Status	Site name			Purchased licenses	Advance Package
	Lori's CMS			100	Purchased package
	Active Server			100	Purchased package
	Total (MAC license excluded)	8 (Free:32)	0	200	

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.



Activate complimentary or purchased licenses manually without an Internet connection.

Follow three steps to activate:

1. Export license request file

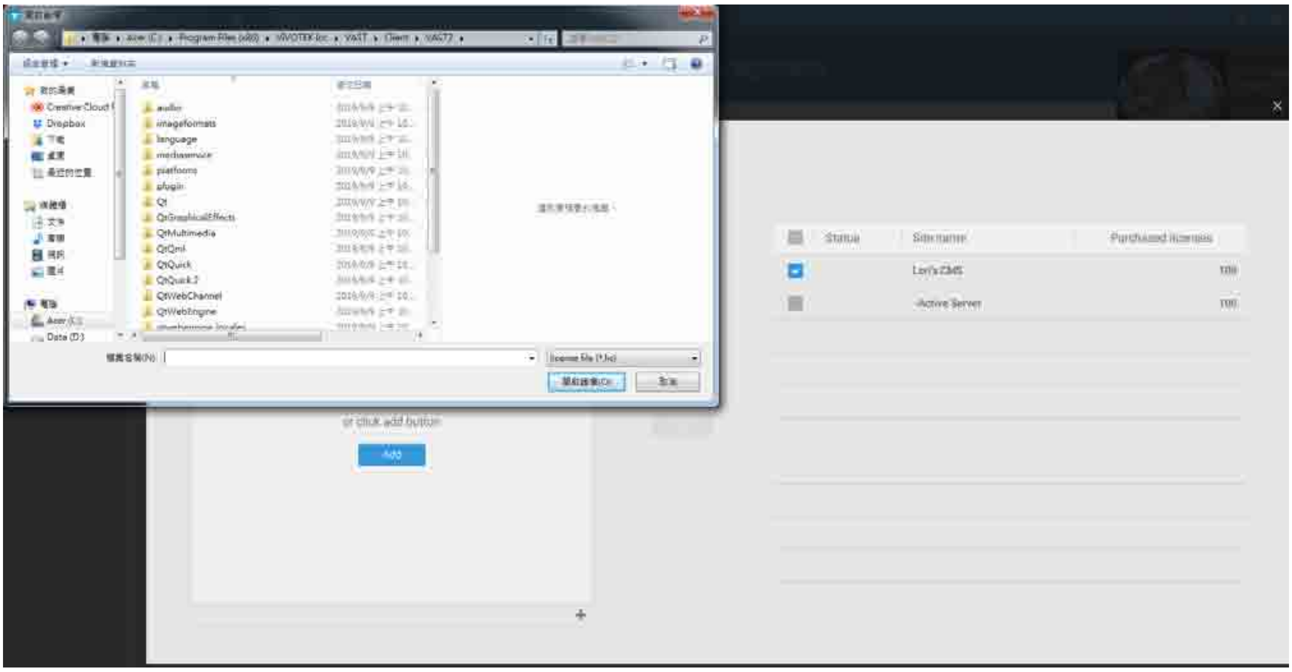
2. Generate license file

Upload license request file to license activation portal

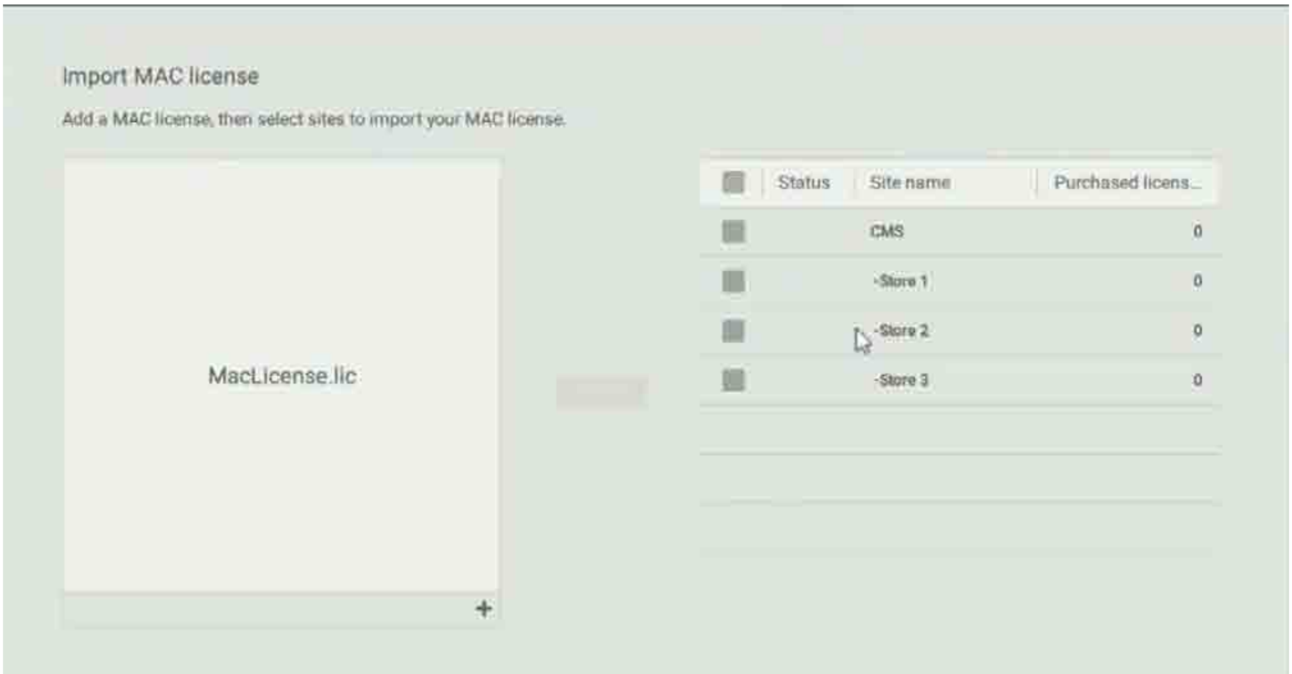
Follow the instruction on the portal and download generated license file

3. Import generated license file

1-6. Select the license file.



1-7. The selected file appears on screen.



Import MAC license

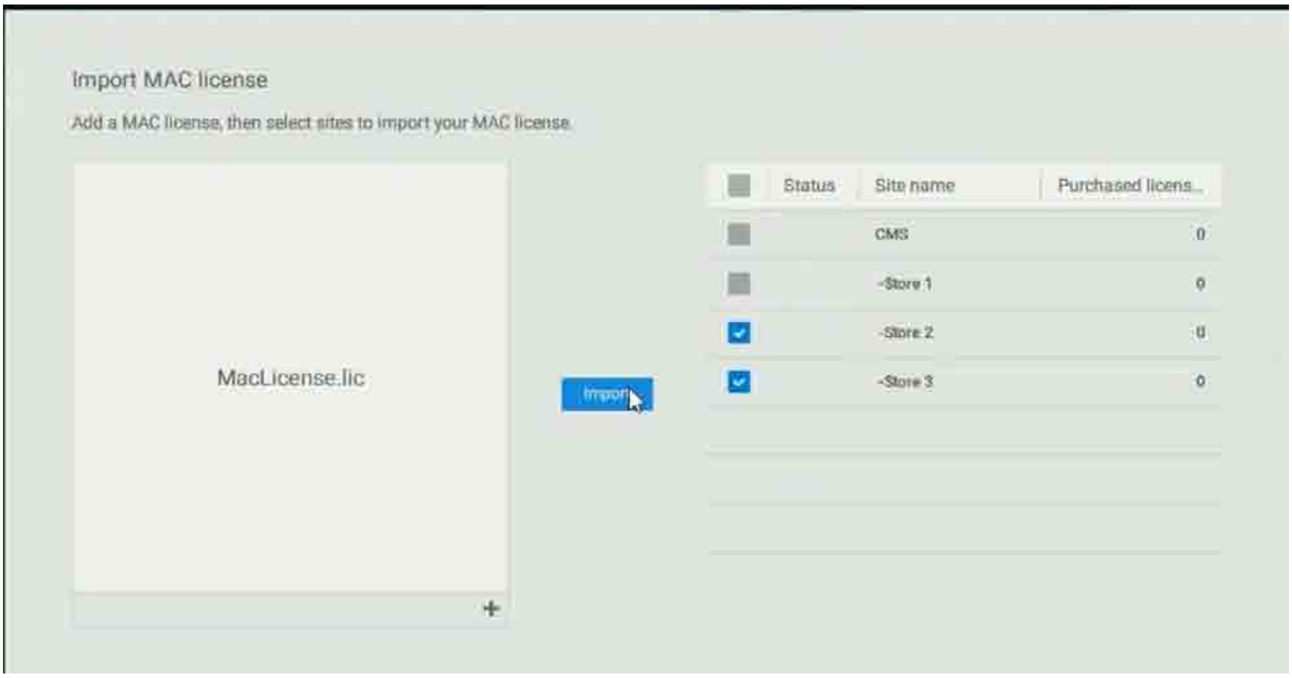
Add a MAC license, then select sites to import your MAC license.

MacLicense.lic

□	Status	Site name	Purchased licens...
□		CMS	0
□		-Store 1	0
□		-Store 2	0
□		-Store 3	0

1-8. Select the target server Stations 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.



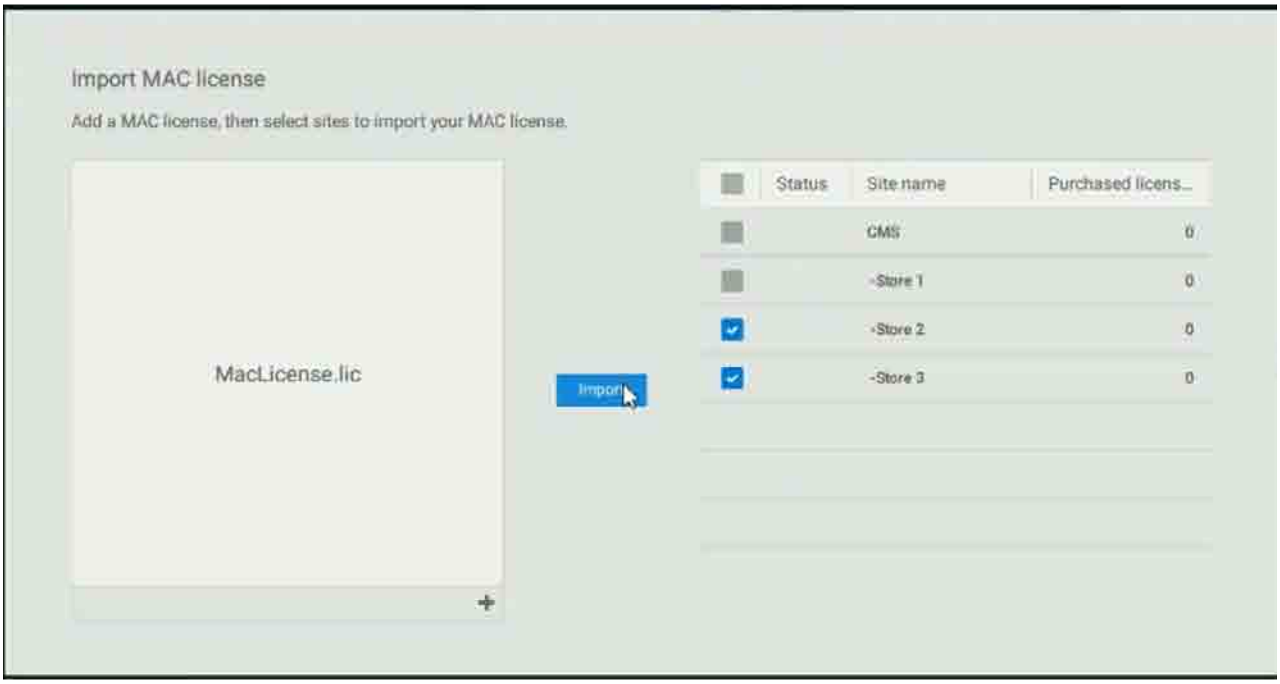
Import MAC license

Add a MAC license, then select sites to import your MAC license.

MacLicense.lic

□	Status	Site name	Purchased licens...
□		CMS	0
□		-Store 1	0
☑		-Store 2	0
☑		-Store 3	0

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



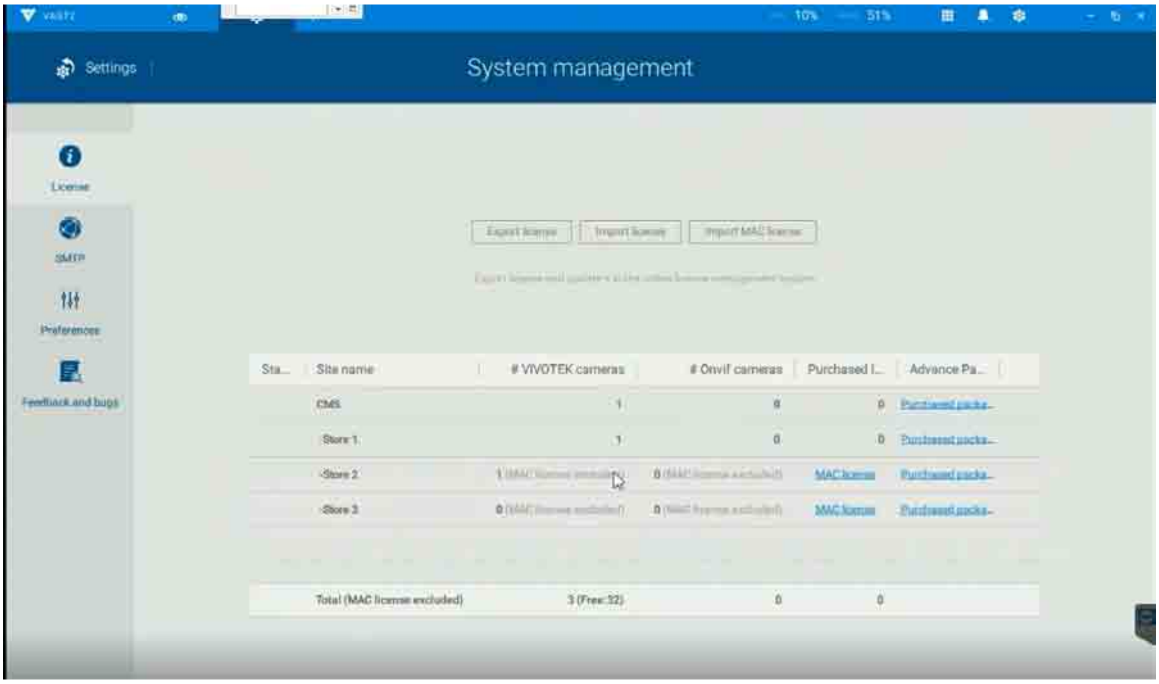
Import MAC license

Add a MAC license, then select sites to import your MAC license.

MacLicense.lic

☐	Status	Site name	Purchased licens...
☐		CMS	0
☐		-Store 1	0
☑		-Store 2	0
☑		-Store 3	0

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



System management

[illegible]

Sta...	Site name	# VIVOTEK cameras	# Onvif cameras	Purchased l...	Advance Pa...
	CMS	1	0	0	Purchased packa...
	Store 1	1	0	0	Purchased packa...
	-Store 2	1 (MAC license excluded)	0 (MAC license excluded)	MAC license	Purchased packa...
	-Store 3	0 (MAC license excluded)	0 (MAC license excluded)	MAC license	Purchased packa...
	Total (MAC license excluded)	3 (Free:32)	0	0	

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

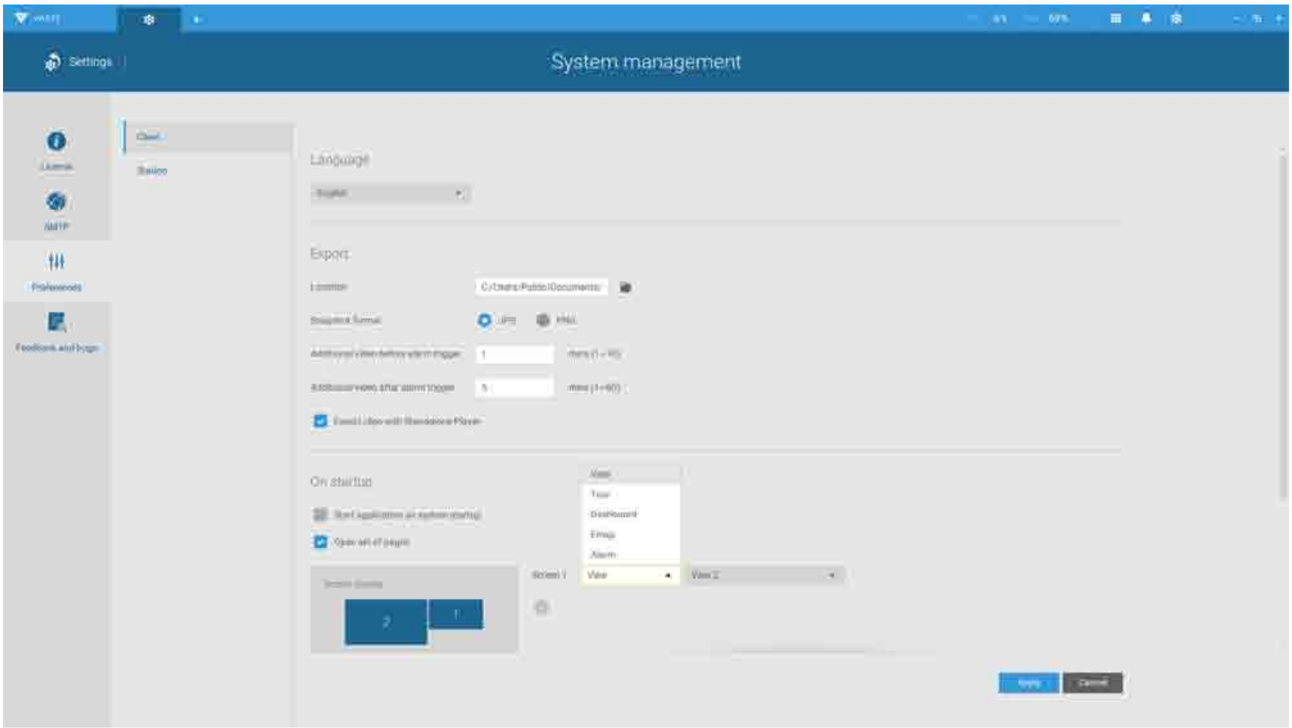
Chapter 4 Settings:

4-1. Settings > System > Preferences

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

Client Setting:

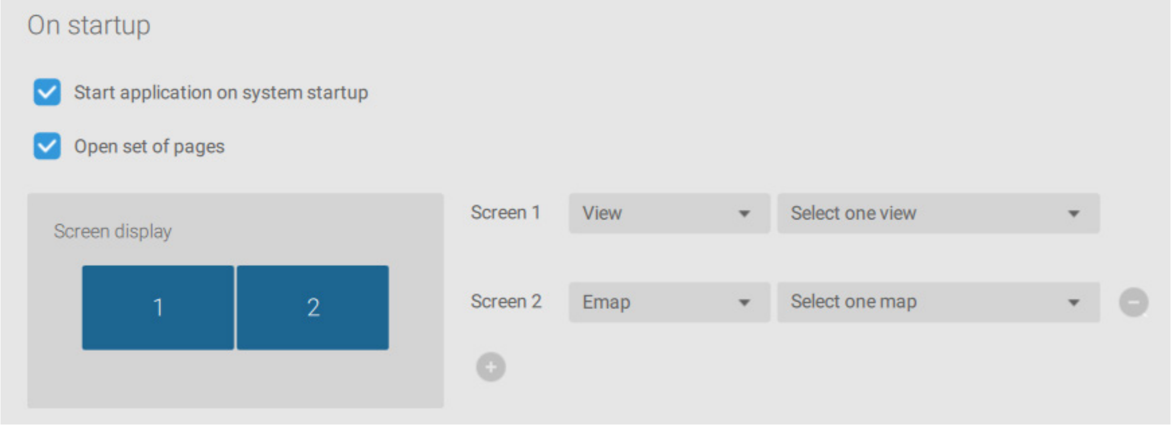
1. Select the UI text language.
2. Configure a default destination for exporting video, snapshots, or configuration backups. The default is "C:\Users\Public\Documents\VIVOTEK Inc\VAST\Downloads". You can change the media format via the checkboxes.
3. Select the format for the snapshot as either JPG or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



6. 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.

Click the Apply button for the configuration to take effect.



On startup

☑ Start application on system startup

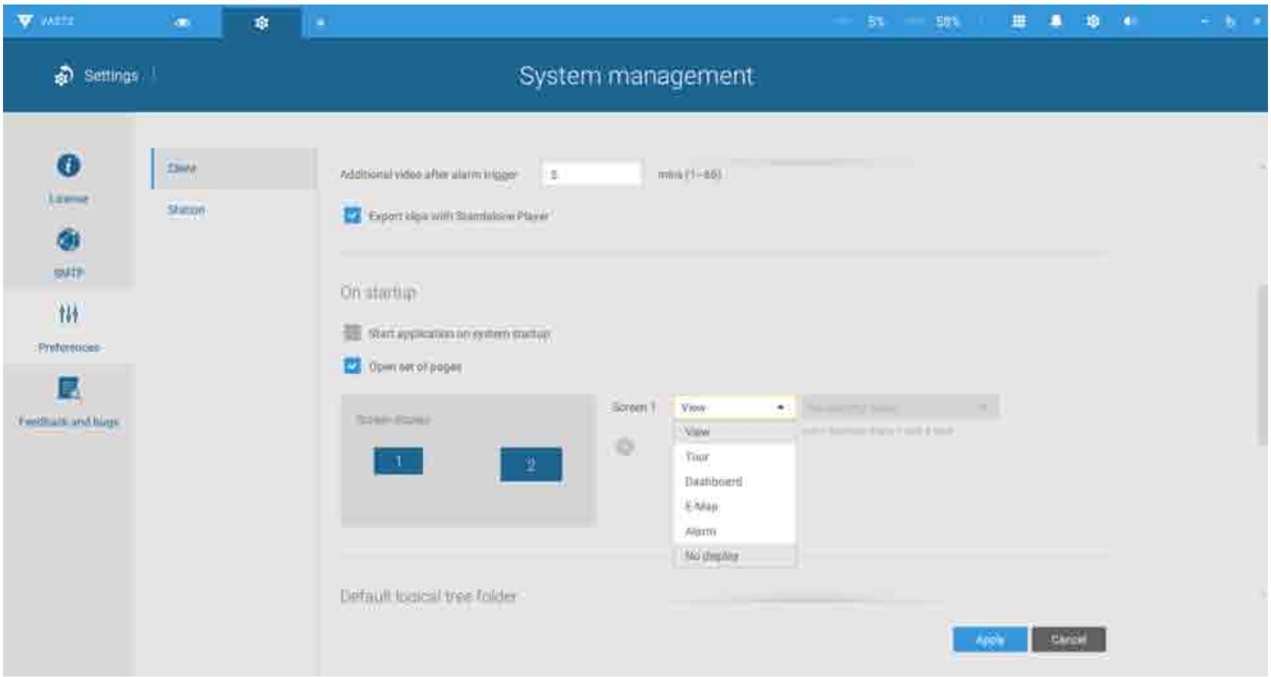
☑ Open set of pages

Screen display

Screen 1: View, Select one view

Screen 2: Emap, Select one map

If you plan to have one monitor to be working for other purposes, select No display for this monitor.



System management

Additional video after alarm trigger: 5 mins (1~60)

☑ Export clips with Standalone Player

On startup

Start application on system startup

☑ Open set of pages

Screen 1: View

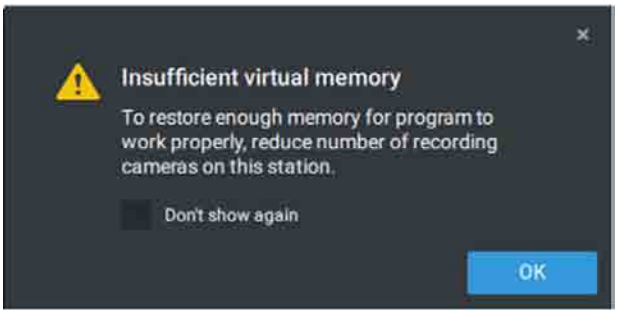
Default logical tree folder

Below are the additional system parameters:

Default logical tree folder: Expanded or collapsed.

Substation streaming connection: CMS Relay or Direct link. Direct link allows a client station to access camera live stream from the sub-station under a CMS main station. CMS relay – A client accesses live stream via the CMS main station.

Show system warning: When a client computer is running short of virtual memory, a warning will display.



Insufficient virtual memory

To restore enough memory for program to work properly, reduce number of recording cameras on this station.

Image resamplig method: Select a resampling method if the need should arise.

Click the Apply button for the configuration to take effect.

Station Setting:

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

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

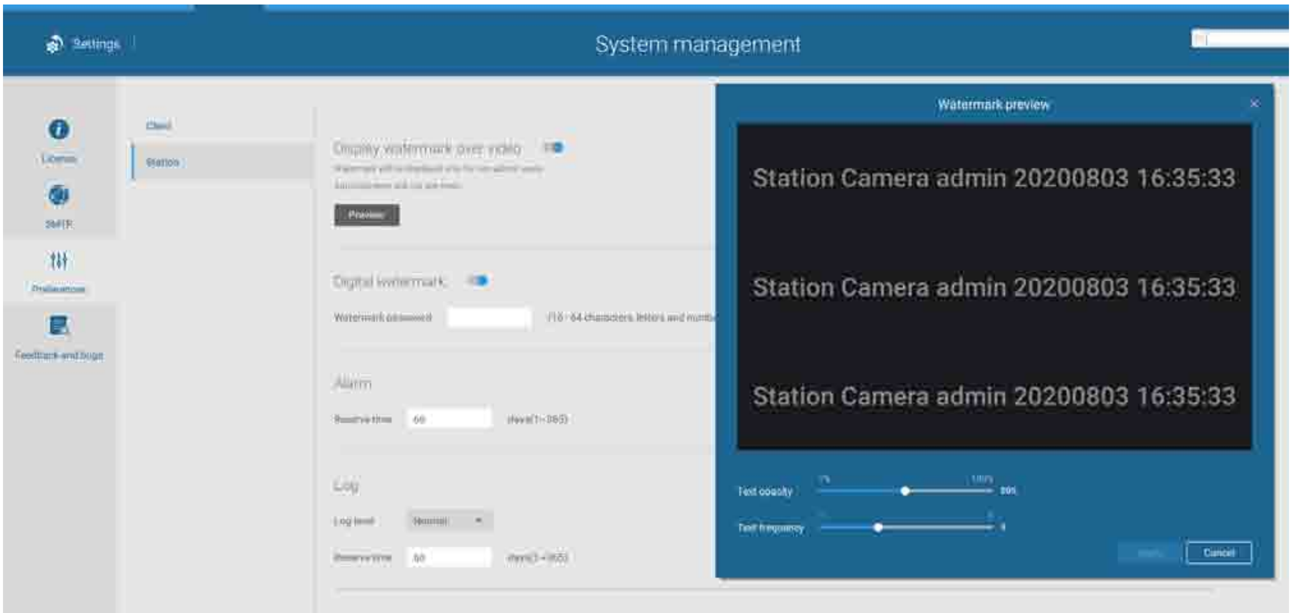
   If enabled, the following will be displayed: camera name + substation name + VAST2 user name + user computer current time. The purpose of watermark is to preserve evidence if the video screen is recorded using cell phones or other devices.

Station Setting:

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

   Note that only non-administrator users will see watermarks.

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



Watermark password (16 - 64 characters, letters and numb

Alarm

Reserve time 60 days(1~365)

Log

Log level Normal

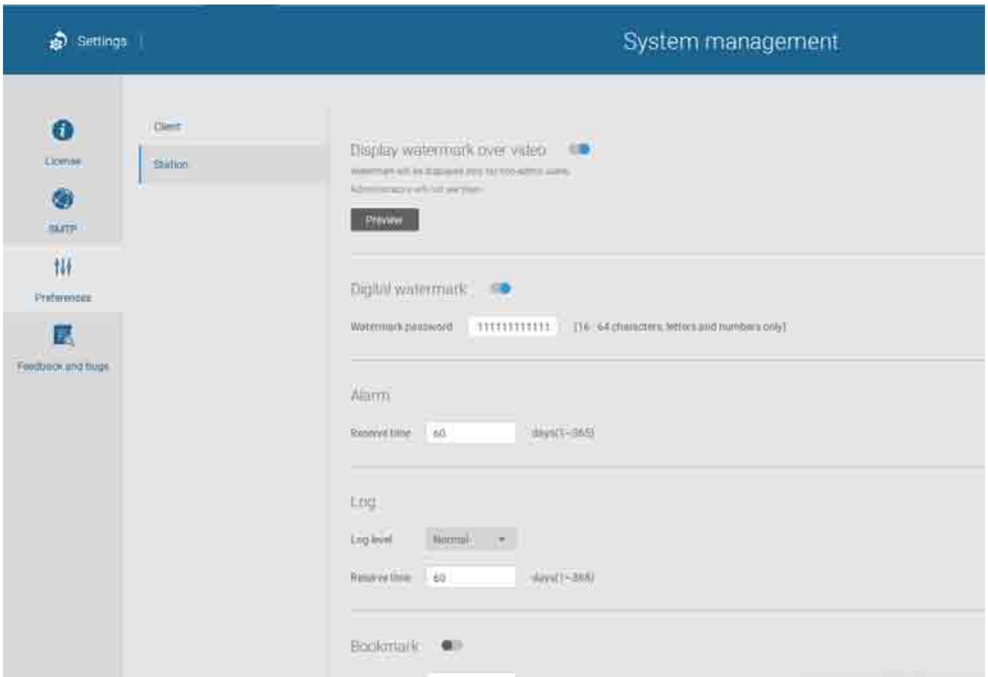
Reserve time 60 days(1~365)

Station Camera admin 20200803 16:35:33

Station Camera admin 20200803 16:35:33

Station Camera admin 20200803 16:35:33

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



Digital watermark

Watermark password 111111111111 [16 - 64 characters, letters and numbers only]

Alarm

Reserve time 60 days(1~365)

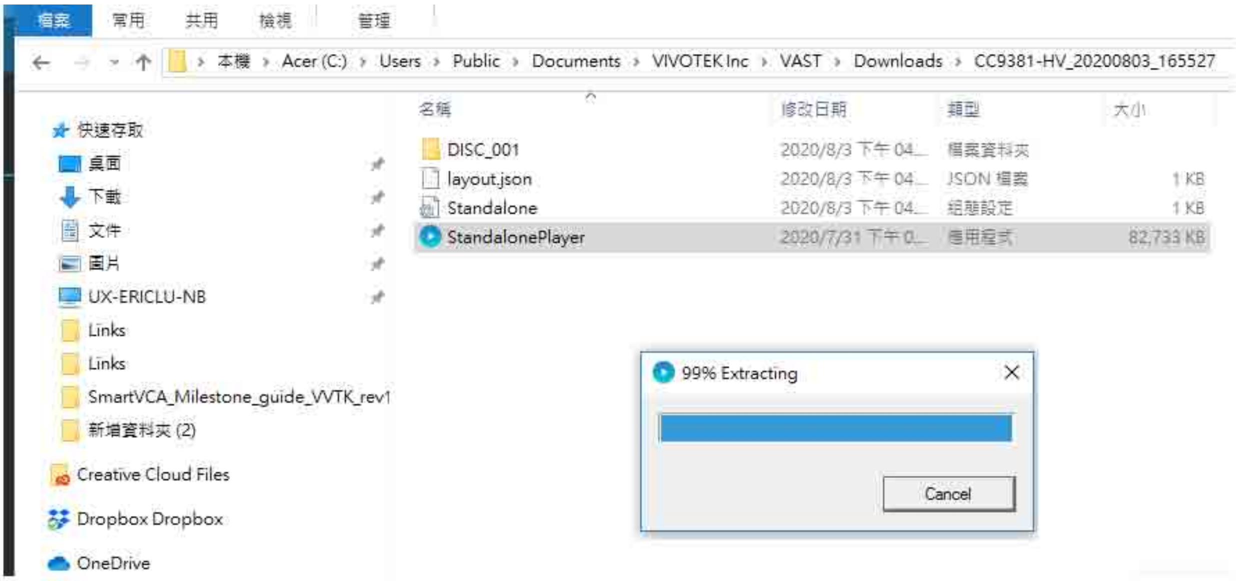
Log

Log level Normal

Reserve time 60 days(1~365)

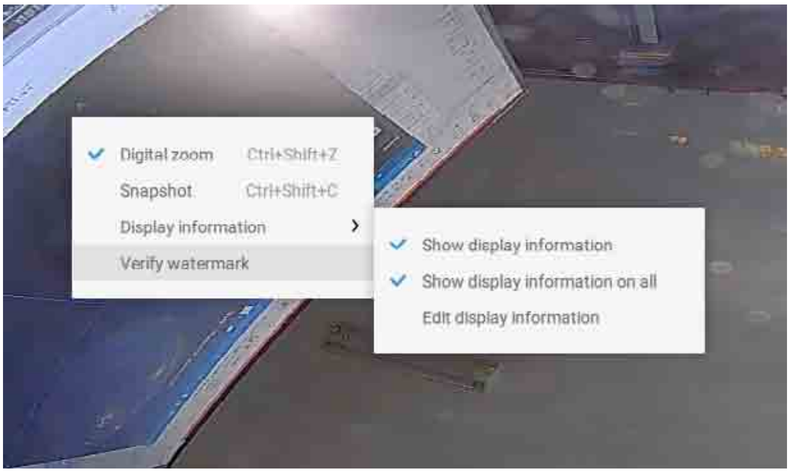
Bookmark

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



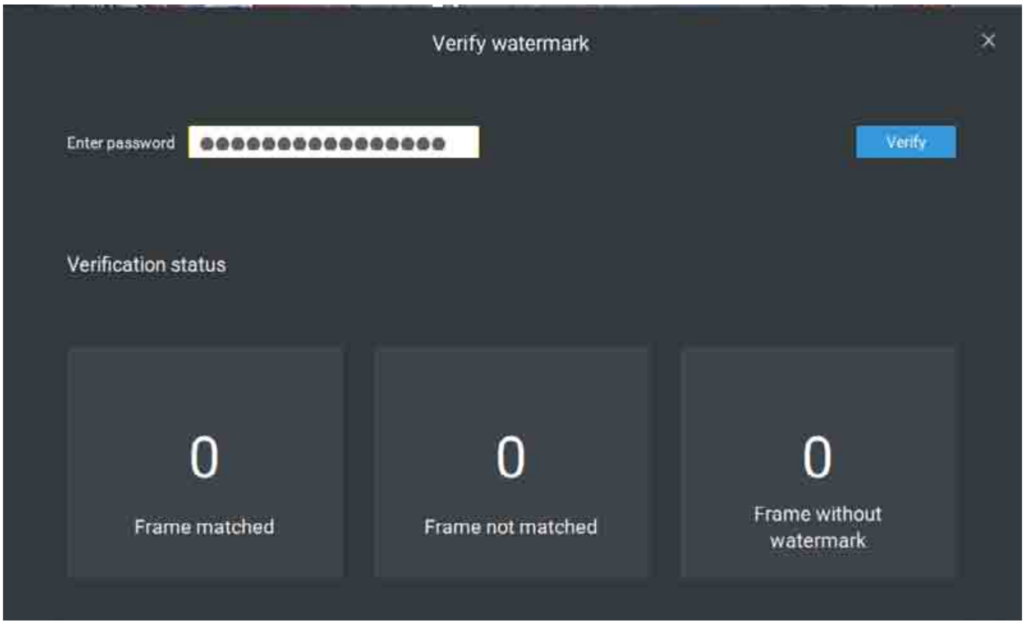
名稱	修改日期	類型	大小
DISC_001	2020/8/3 下午 04...	檔案資料夾	
layout.json	2020/8/3 下午 04...	JSON 檔案	1 KB
Standalone	2020/8/3 下午 04...	組態設定	1 KB
StandalonePlayer	2020/7/31 下午 0...	應用程式	82,733 KB

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



✓ Digital zoom Ctrl+Shift+Z
Snapshot Ctrl+Shift+C
Display information ›
Verify watermark
✓ Show display information
✓ Show display information on all
Edit display information

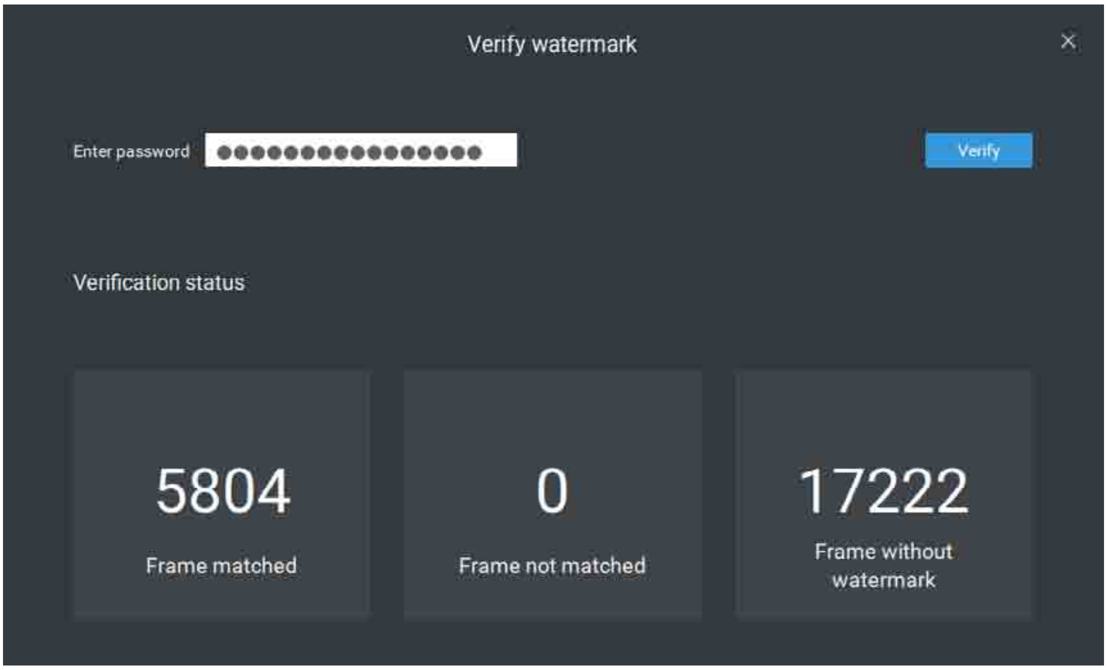
The Verify screen will display. Enter the pre-configured password. Click Verify.



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

Frame matched: Your video was exported with the digital password, and you entered the correct password.
Frame not matched: Your video was exported with the digital password, and you entered the incorrect password.
Frame without watermark: a. If your video wasn't exported with the digital password.
b. If your video was exported with the digital password, and your video has been tampered.

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

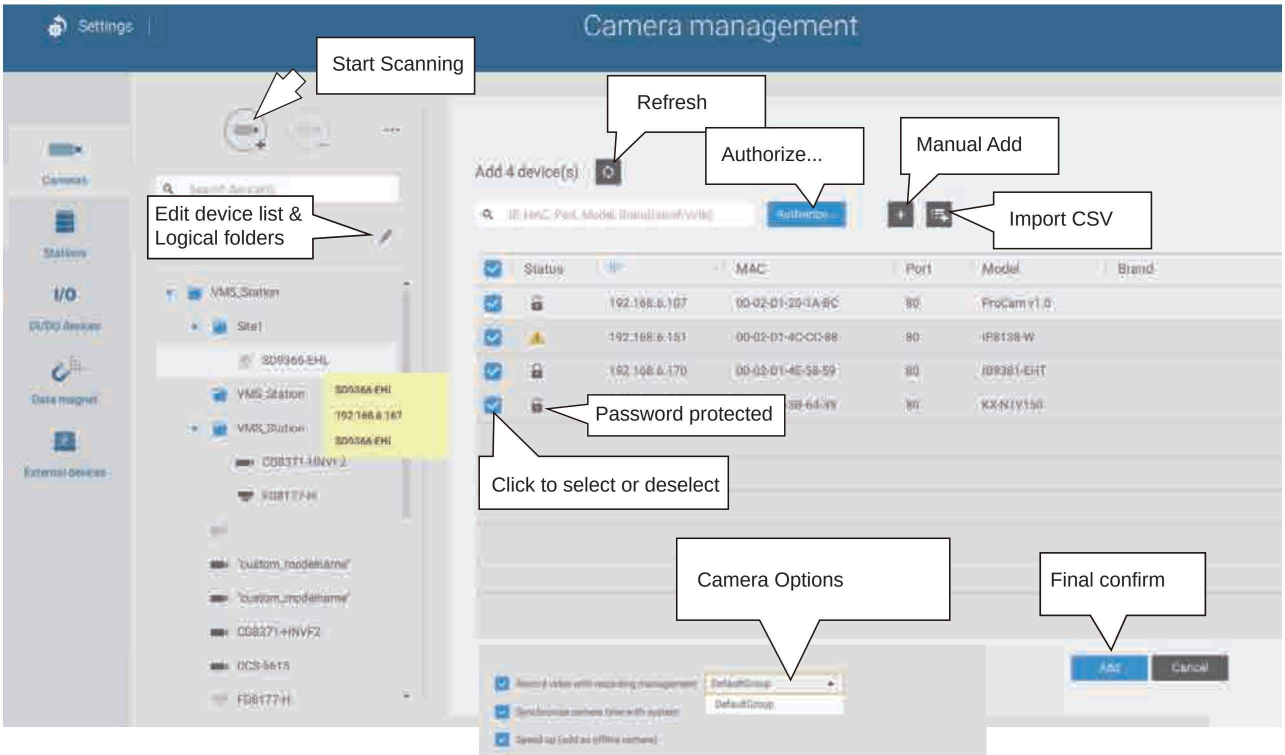


3. **Alarm** - Reservation time: Configure the preservation time of the alarms and logs. Note that some alarms can be triggered with recorded videos. Configuring a preservation time can help reduce the use of storage space on server.
4. **Log**: Use the menu to configure the preservation time of the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

4-2. Settings > Device > Cameras

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

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



Add 4 device(s)

☑	Status	IP	MAC	Port	Model	Brand
☑	🔓	192.168.6.107	00-02-D1-20-1A-BC	80	ProCam v1.0	
☑	⚠	192.168.6.151	00-02-D1-4C-CC-88	80	IP8138-W	
☑	🔒	192.168.6.170	00-02-D1-4E-58-59	80	IB9381-EHT	
☑	🔓	[illegible]	[illegible]-5B-64-49	80	KX-N1V150	

☑ Record video with recording management DefaultGroup
☑ Synchronize camera time with system
☑ Speed up (add as offline camera)

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.

Record video with recording management: You can decide which recording group to record the videos to using a pull-down menu.

Speed up (add as offline cameras): Normally, you should have all the credentials for the access to all network cameras. However, in the condition that you add a large number of cameras using the "import devices from device list" function, you can temporarily use this speed up option to add these cameras.

This appllies when the cameras have not been installed (have been prepared for installation), but you want to add them to the camera list. When cameras have all been installed, VAST will attempt to connect with them.

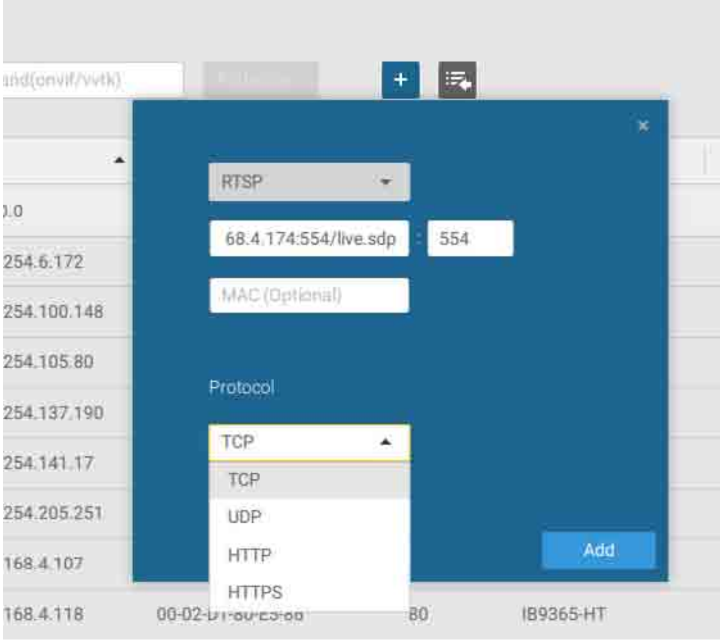
- Retrieve RTSP streaming on specific port: The default port for RTSP streaming is 554. If you want to change this port, please check this item and fill in a desired port number.

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. The feature enables the support for obsolete models.

To insert a camera using the URL-like command,

1. Select the camera Brand as "**RTSP**."



RTSP

68.4.174:554/live.sdp : 554

MAC (Optional)

Protocol: TCP

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.

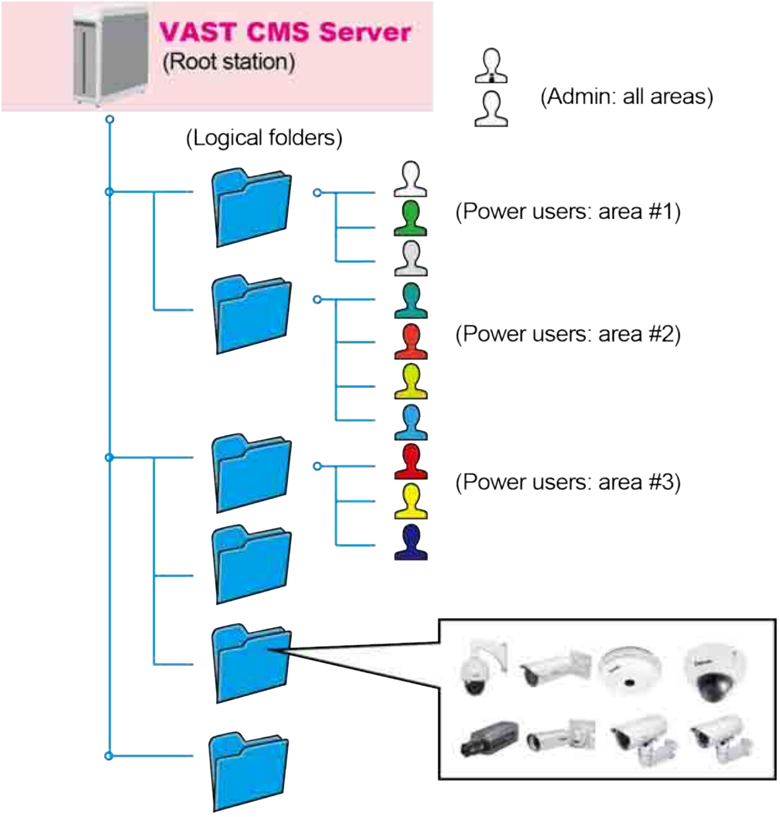
6. Select a preferred protocol.

   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.

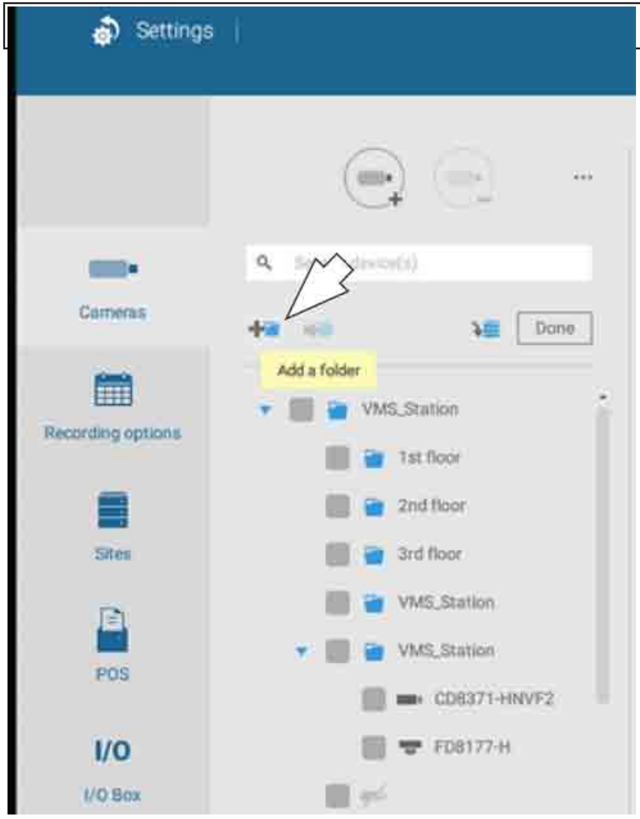
4-3. Logical Folders

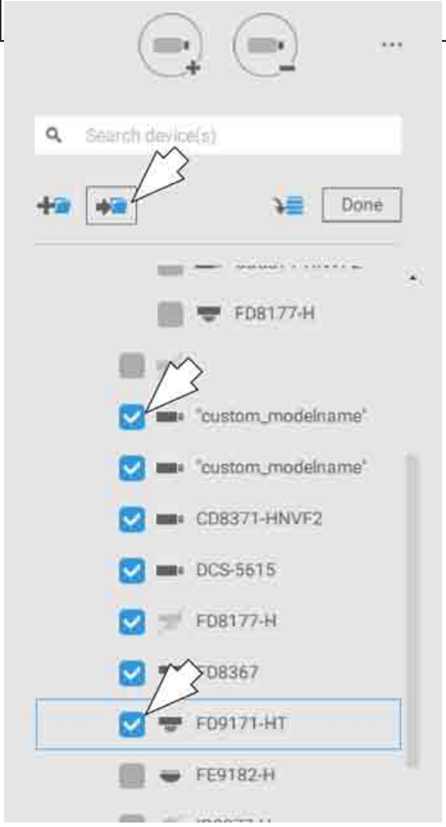
The Logical Folders allow you to re-define the logical relationships between the real-world deployment and the physical devices (cameras). For example, according to your deployments, you can designate several cameras to be listed under a logical sub-directory named as "Building A," and the other cameras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



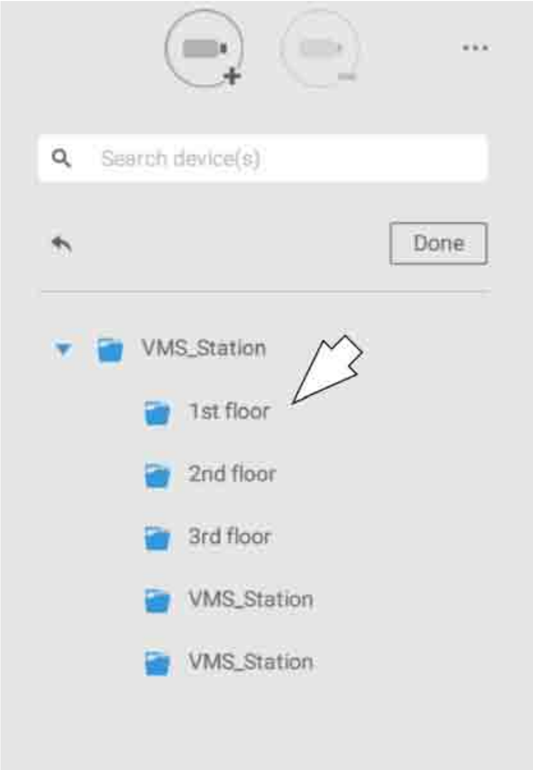
To create logical folders,

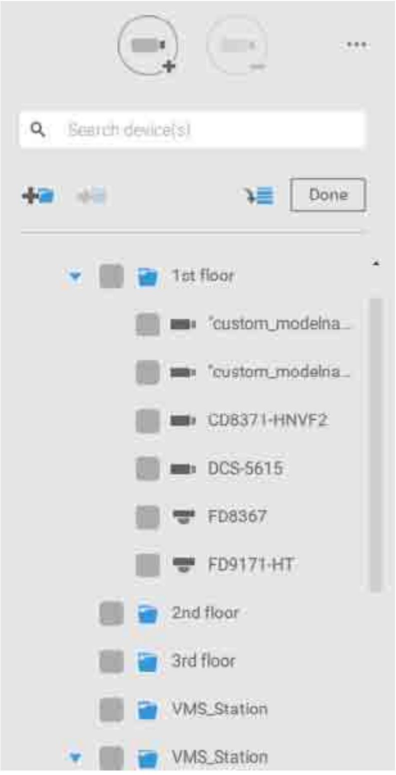
1. On the Settings > Cameras page, click the Edit ✎ button.
2. Click on the Add a folder button.
3. Enter a name for the folder, e.g., 1st floor, 2nd floor,... according to your needs as shown below.
4. Repeat the process to create more folders.
5. Make sure you enlisted all cameras in your deployment.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



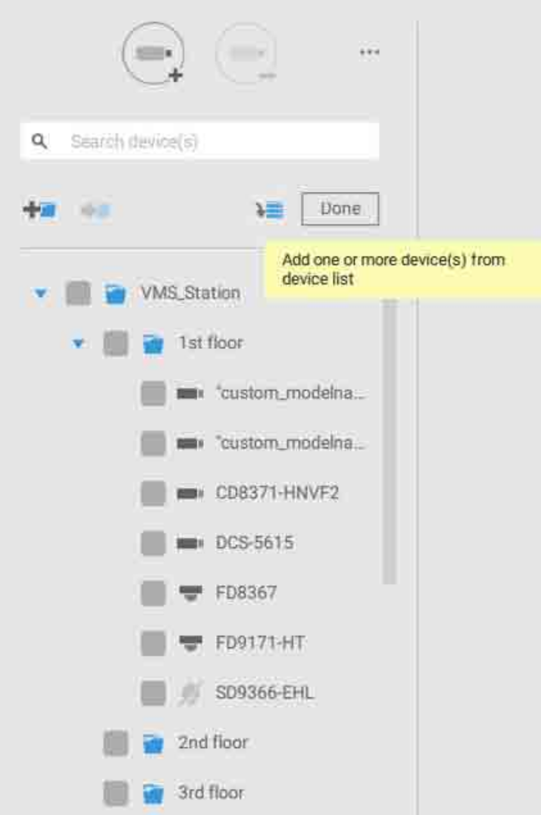


6. Select a logical folder to move the devices to. The selected devices will be listed under the logical folder you selected. Repeat the process to move cameras to each logical folder.

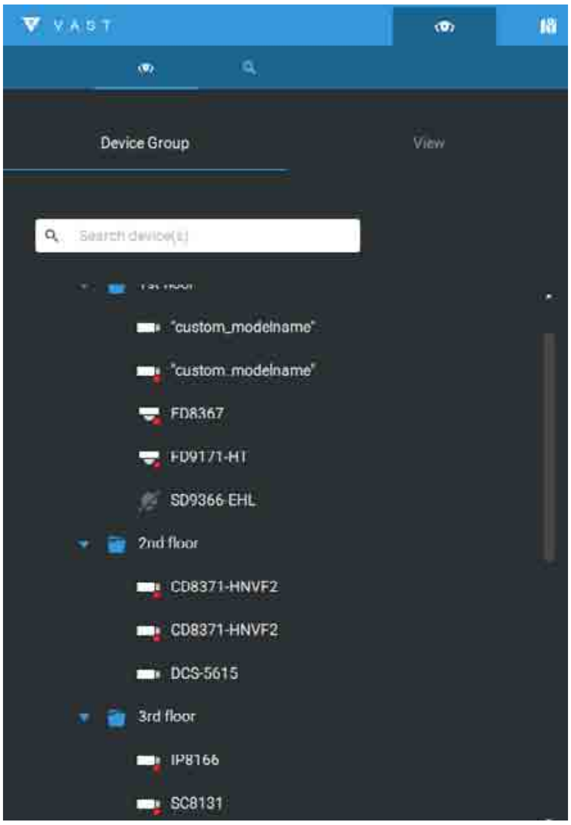




You can also use the add device button to select devices from the list and move them to a specific folder.



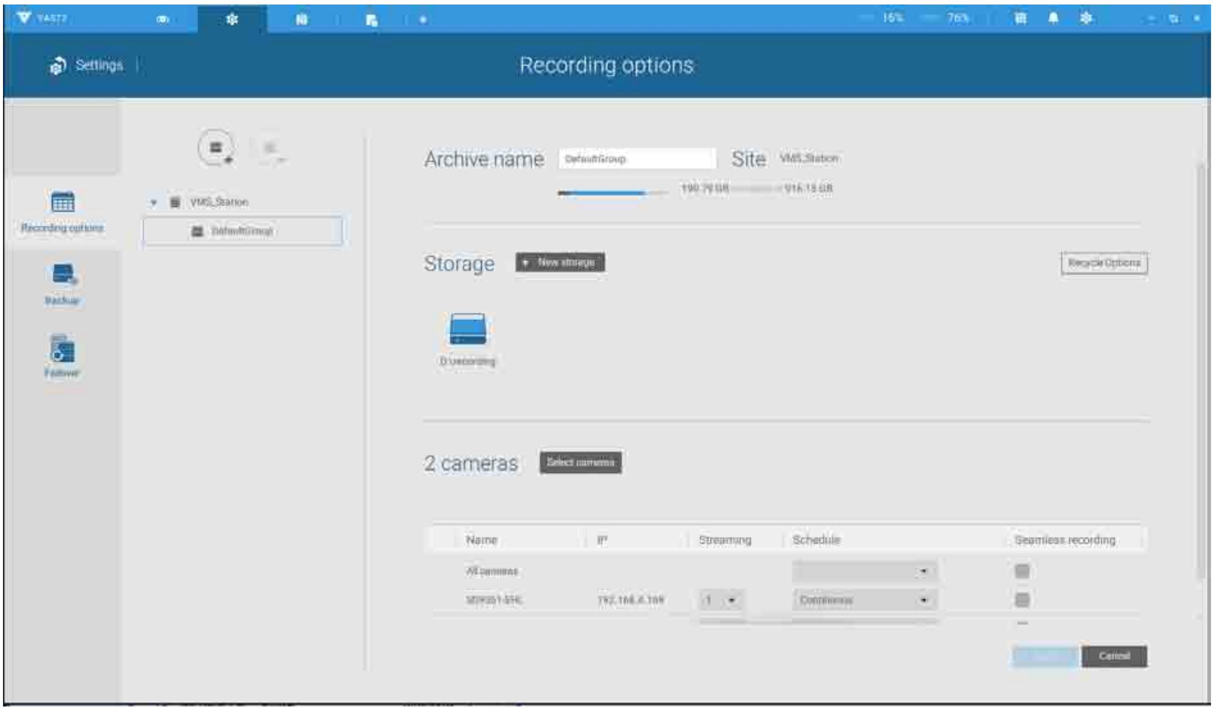
Return to live view, and you can see the configuration change takes effect.



4-4. Settings > Recording > Recording Options

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

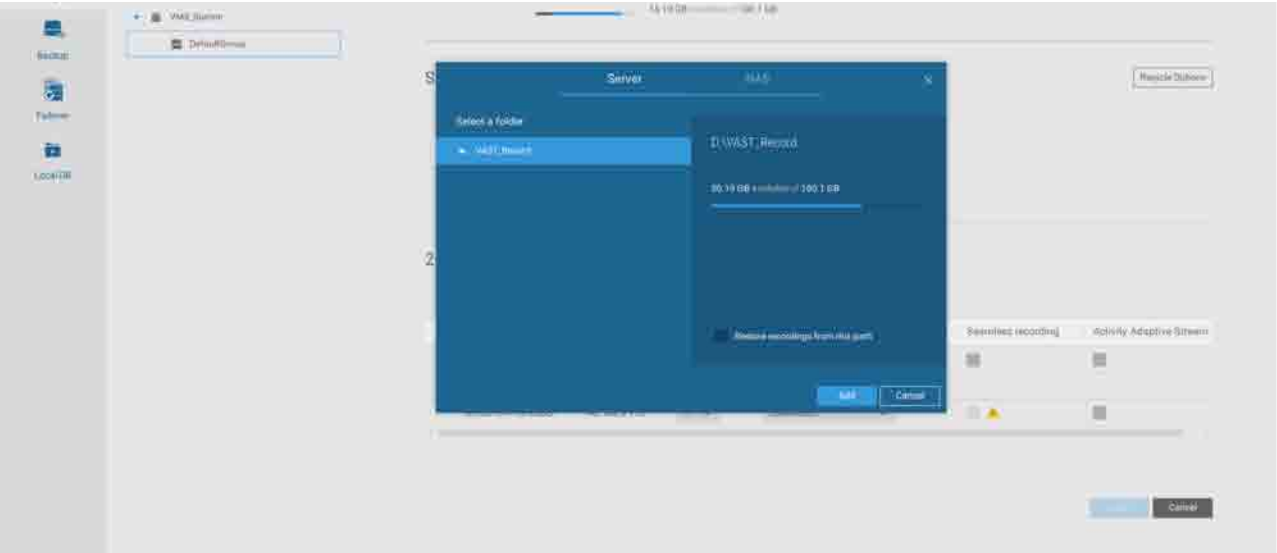
You can configure recording schedules or select the storage options, including the configuration of an external NAS storage. You can designaate a recording folder of your choice.



Archive name: DefaultGroup Site: VMS_Station

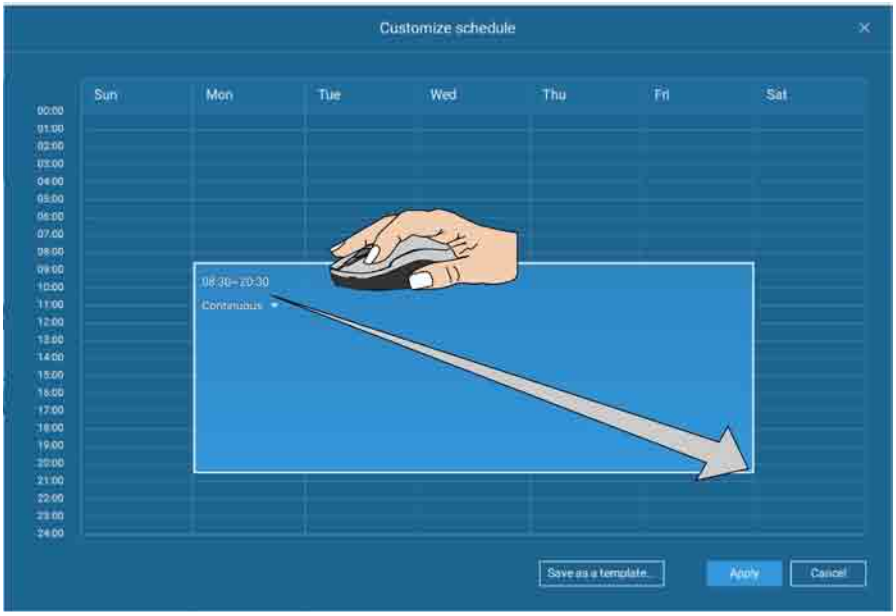
190.79 GB / 916.15 GB

Name	IP	Streaming	Schedule	Seamless recording
All cameras				□
SD9351-EHL	192.168.4.169	1	Continuous	□



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.

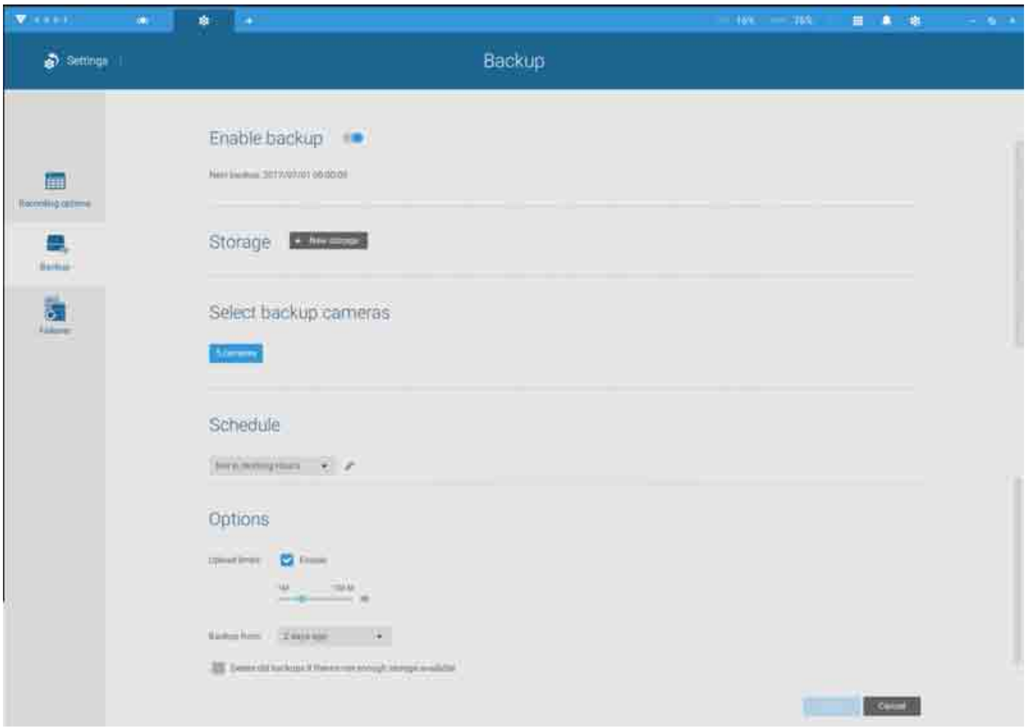
The same configuraion window apply to both the Schedule template and the customize schedule windows.

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.



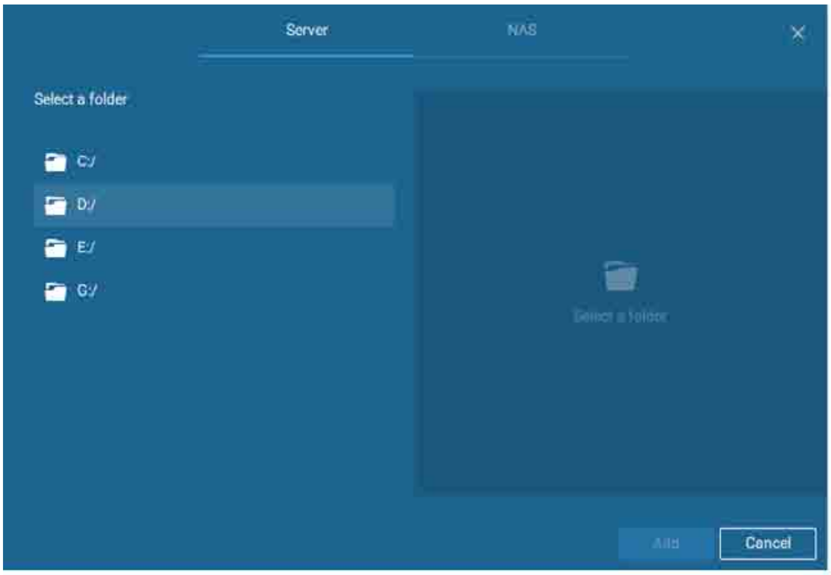
Next backup: 2017/07/01 06:00:00

Upload limit ☑ Enable

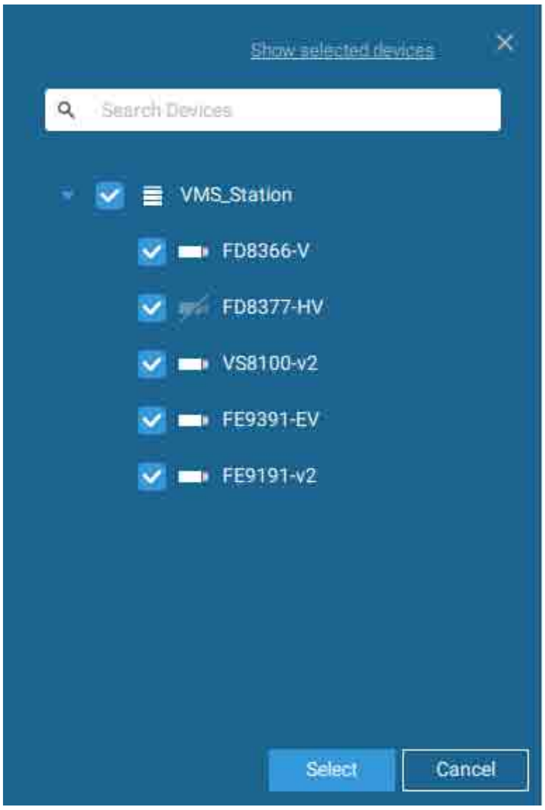
Backup from: 2 days ago

To enable a backup schedule,

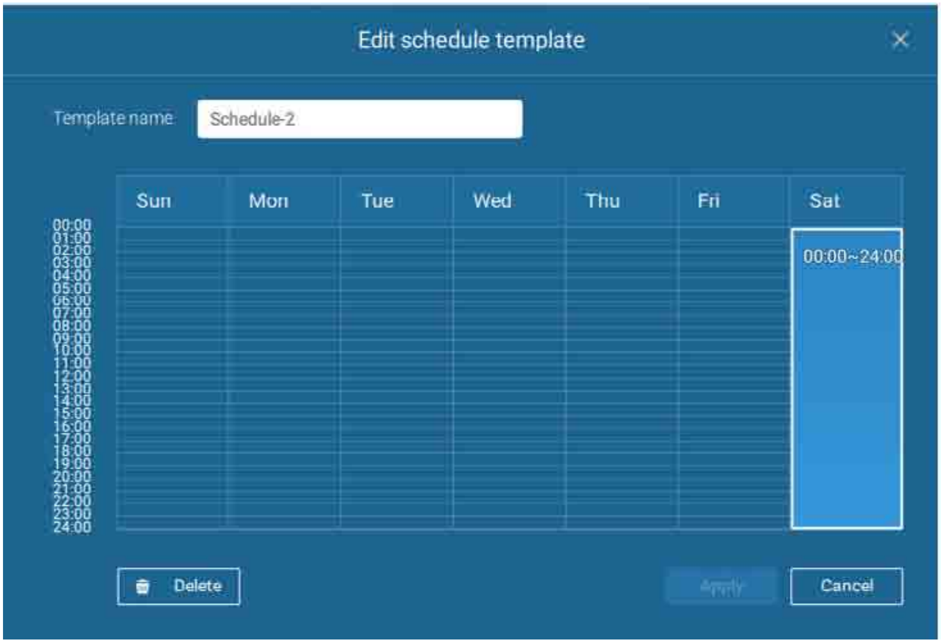
1. Enable the backup by selecting the "Enable backup" slide switch.
2. Click to add New storage. A configuration window will prompt showing all accessible storage. Click the NAS tab to enable access to a network share.



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.



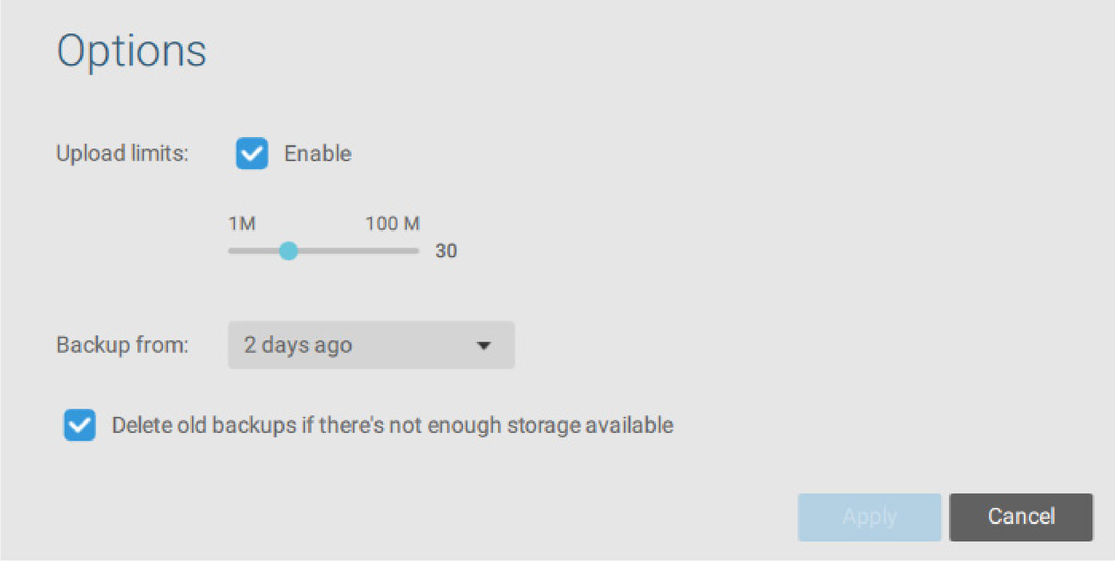
Edit schedule template

Template name: Schedule-2

Sat: 00:00~24:00

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

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



Options

Upload limits: ☑ Enable

1M 100 M 30

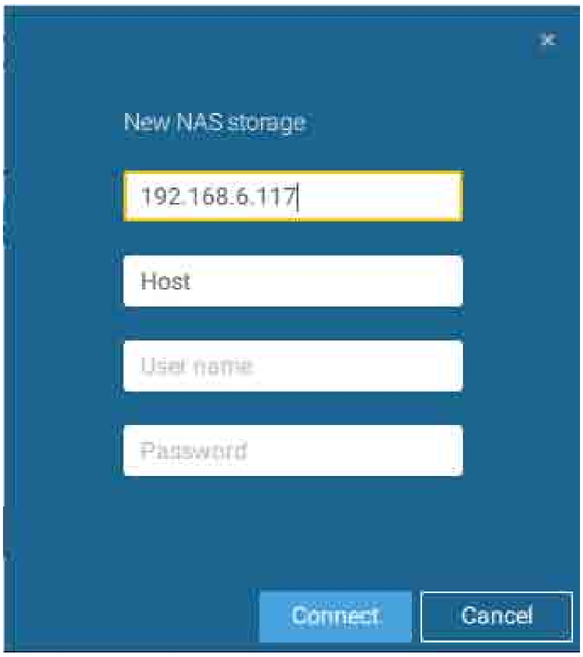
Backup from: 2 days ago

☑ Delete old backups if there's not enough storage available

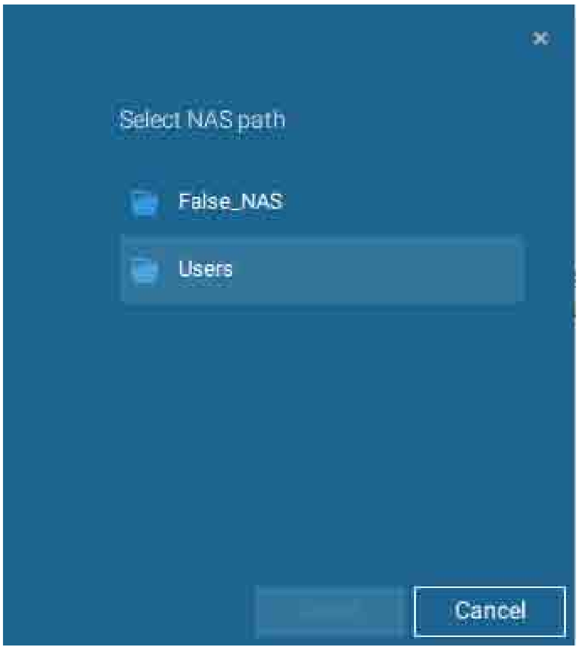
Storage

By default, VAST will check if 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 shared volumes 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.



192.168.6.117



Select storage volumes each by a single click.

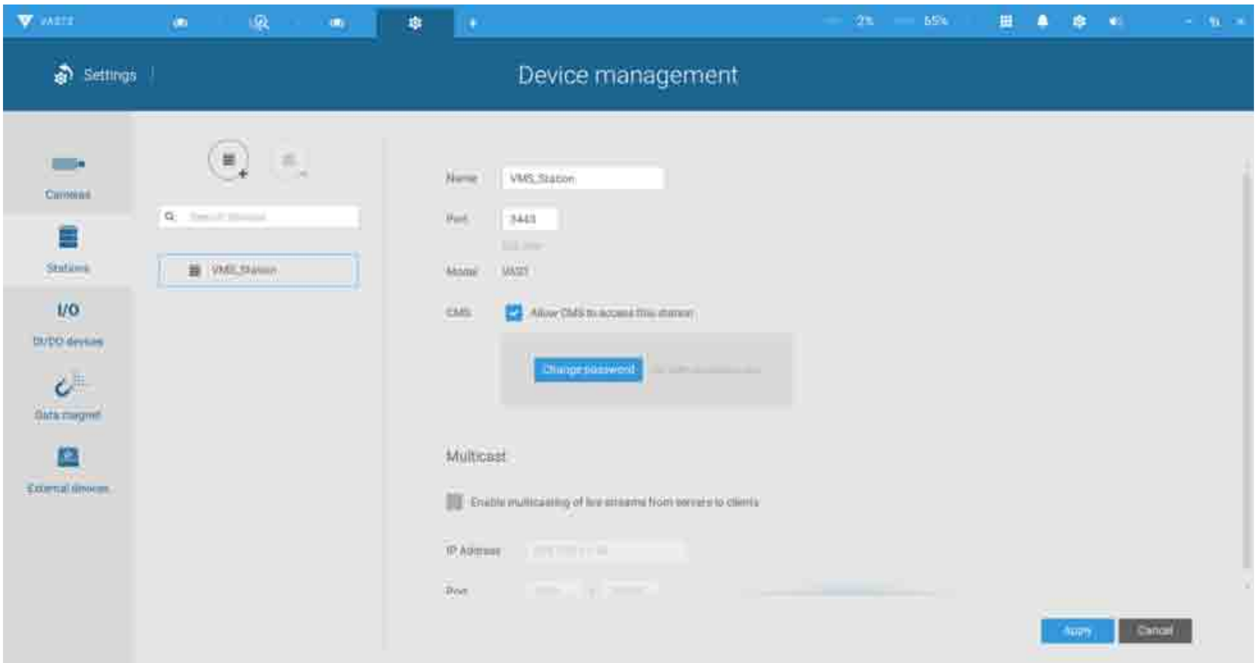
Click **Ready to use** to continue.

4-6. Settings > Device > Stations

The VAST2 allows a deployment consisting of multiple VAST instances at different locations. 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 substation.
2. Enter Settings > Stations.
3. Enter a TCP Port number if your network configuration requires a different port.
4. Select Allow CMS to access this station.
5. Click Change password. This password will be used to authenticate the connection between a CMS VAST server and substations.



Name: VMS_Station

Port: 3443

Model: VAST

CMS: ☑ Allow CMS to access this station

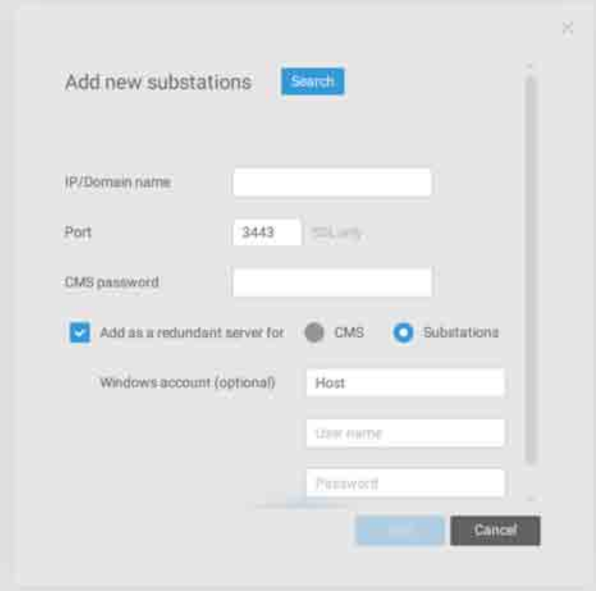
□ Enable multicasting of live streams from servers to clients

6. Click the Apply button.

7. Open the VAST 2 client on the server chosen as the CMS.

8. Click the **Add substations** button.

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



Add new substations

IP/Domain name:

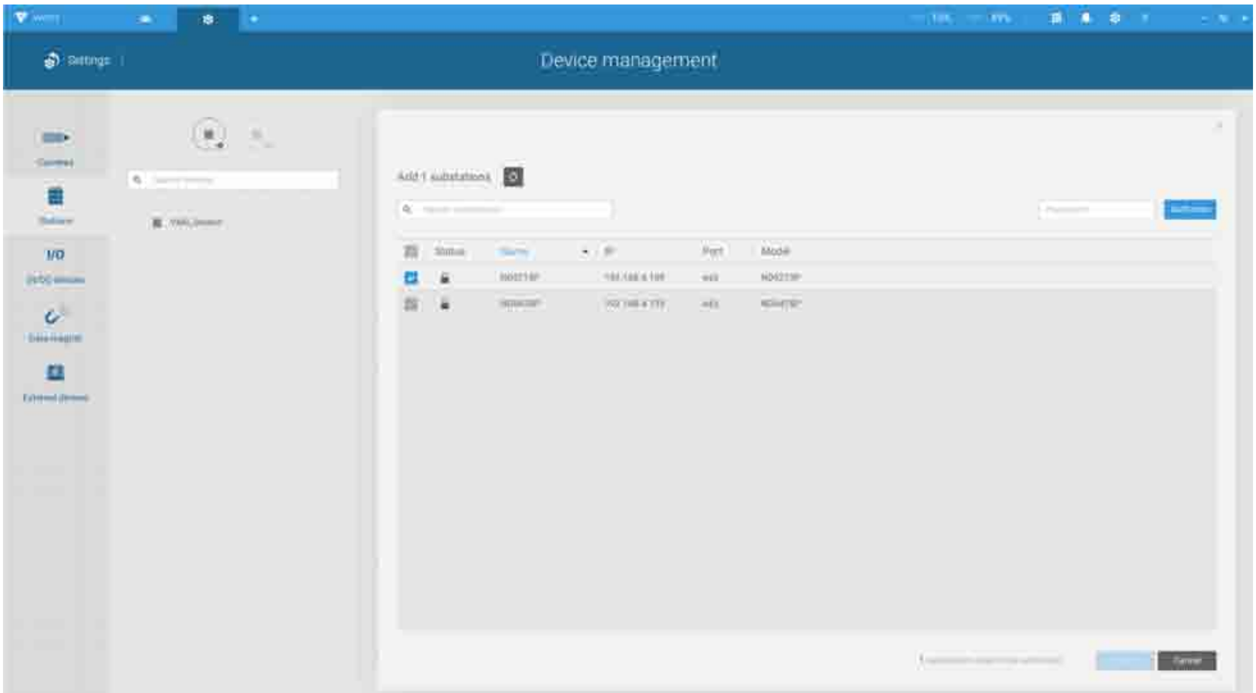
Port: 3443

CMS password:

☑ Add as a redundant server for ● CMS ○ Substations

Windows account (optional): Host

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

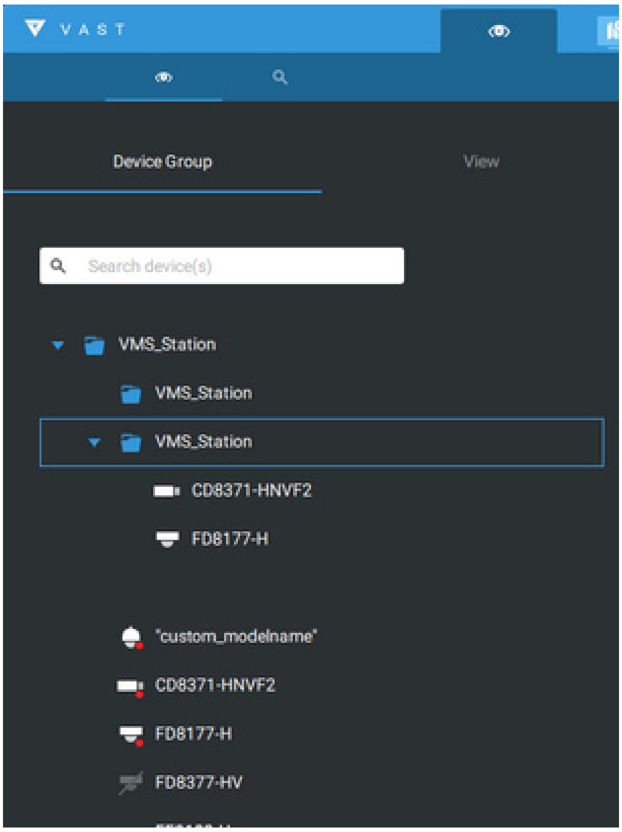


Device management

Add 1 substations

	Status	Name	IP	Port	Model
☑	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
□	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

The substations and its subordinate devices should be immediately listed under the CMS station. You can create separate views to place the substations' cameras.

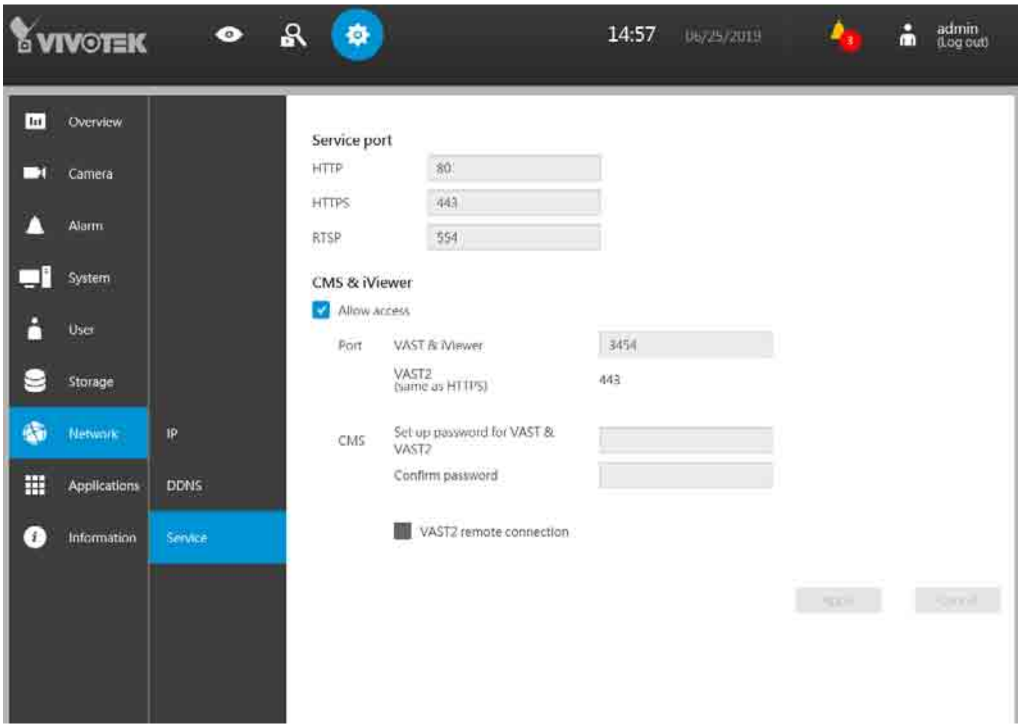


- VMS_Station
  - VMS_Station
  - VMS_Station
    - CD8371-HNVF2
    - FD8177-H
  - "custom_modelname"
  - CD8371-HNVF2
  - FD8177-H
  - FD8377-HV

When you want to enlist an NVR into your configuration, please remember to enable the access from VAST server in the NVR's **Service** page.

The connection between VAST and NVR is made via encrypted https.

If the connection port is changed to a non-SSL port, the access from VAST to NVR will fail. For adding the ND series NVR, use port **443**.



Service port

HTTP	80
HTTPS	443
RTSP	554

CMS & iViewer

☑ Allow access

Port	VAST & iViewer	3454
	VAST2 (same as HTTPS)	443
CMS	Set up password for VAST & VAST2	
	Confirm password	

□ VAST2 remote connection

Multicasting

The VAST2 supports multicasting of live streams from server to clients. If multiple VAST2 clients demand live videos from the same camera, multicasting cna help save considerable system resources.

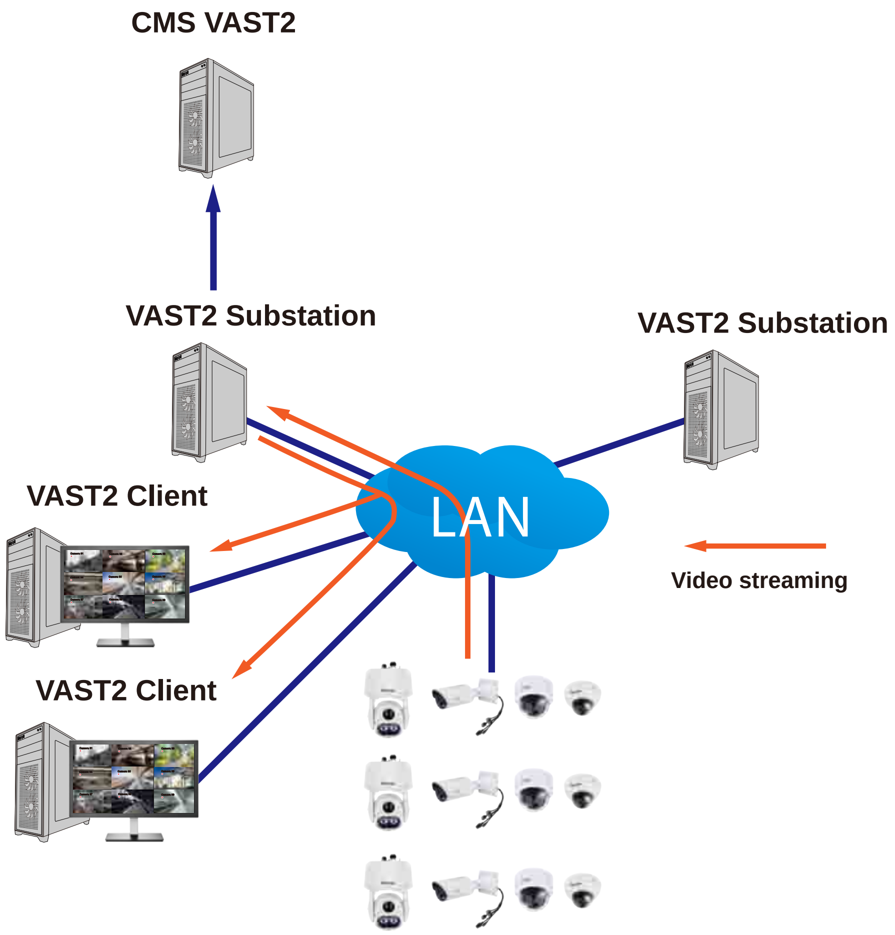
Multicasting should be enabled on a VAST server and also on individual cameras.

There are prerequisites:

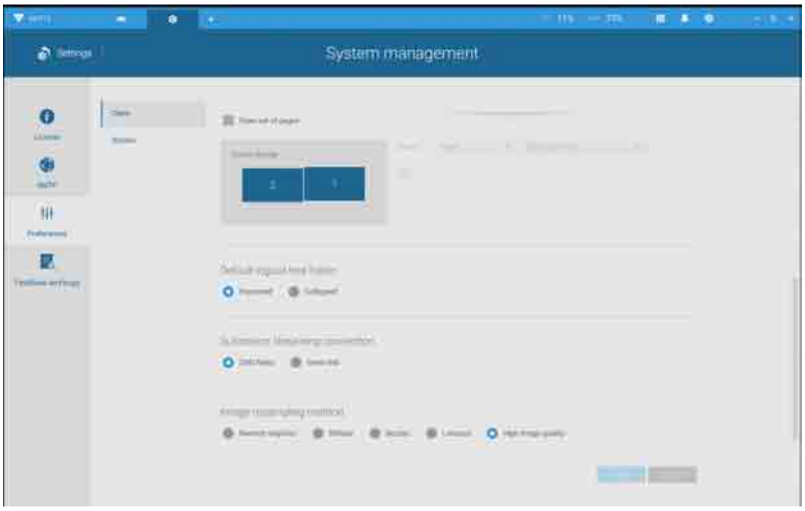
1. Both the VAST2 server and clients have to be revision 2.7 or above. If any of them is running revisions before 2.7, client connections will crash.
2. Multicasting is not supported under the following conditions:

* A CMS local client can only access the live stream from the cameras managed by the CMS server using unicast connections.

* If the need arises for access to cameras managed by VAST sub-stations, the multicasting configuration should take place on the sub-stations instead of on the CMS server.



* If the streaming connection for a sub-station is configured as **CMS Relay**, you should configure the multicasting settings on the CMS server.

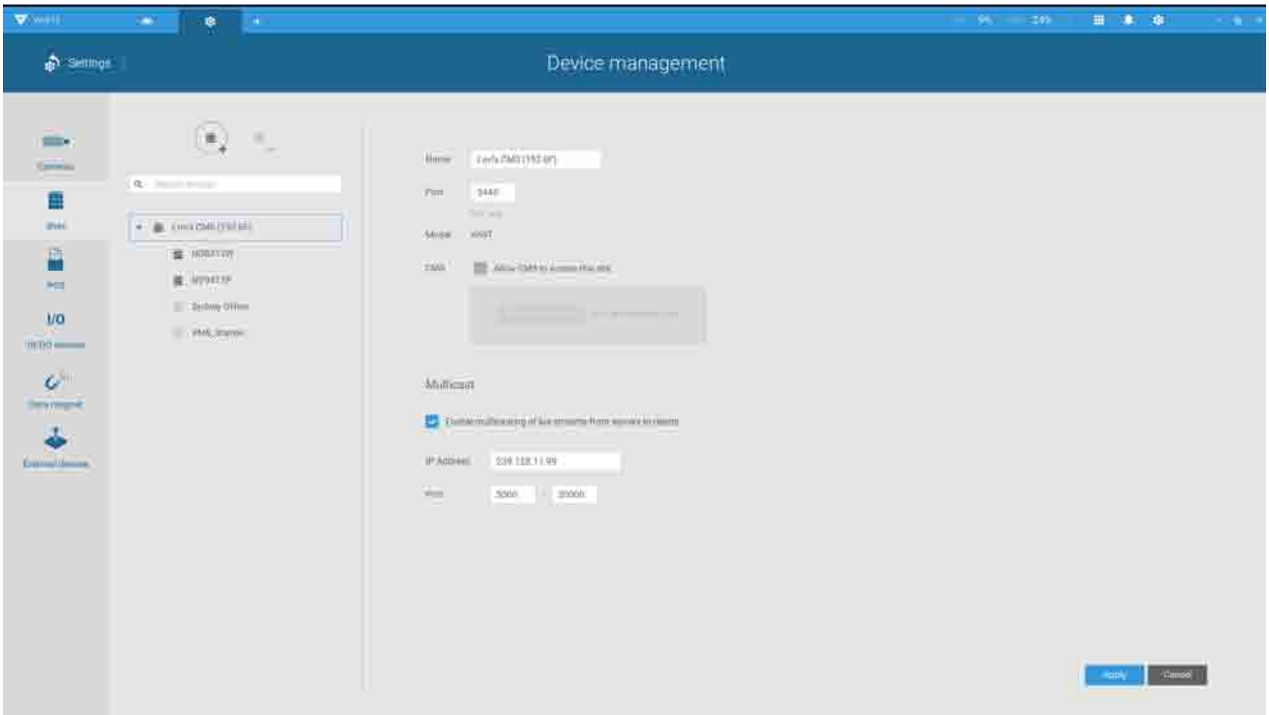


* To enable multicasting, your network infrastructure must support the IP multicasting standard IGMP (Internet Group Management Protocol). Your server and clients should be on the the same network segment.
* Multicasting is only possible for live streams, not applicable to the recorded video or audio.
* Multicast streams are not encrypted, even if the the recording server uses encryption.
* The IPv4 multicast address range is: 224.0.0.0 to 239.255.255.255.
* A layer 2 network switch that supports IGMP is required in the configuration.

To enable Multicasting on a VAST server:

1. Enter Settings > Device > Stations.
2. Single-click to select a server for which you want to enable the Multicasting.
3. Click the checkbox to enable the configuration and enter the multicast address.
4. Click the **Apply** button.

Starting the Multicasting service will restart the VAST server.



Name [illegible]

Port 3445

Model VAST

CMS □ Allow CMS to access this site

Multicast

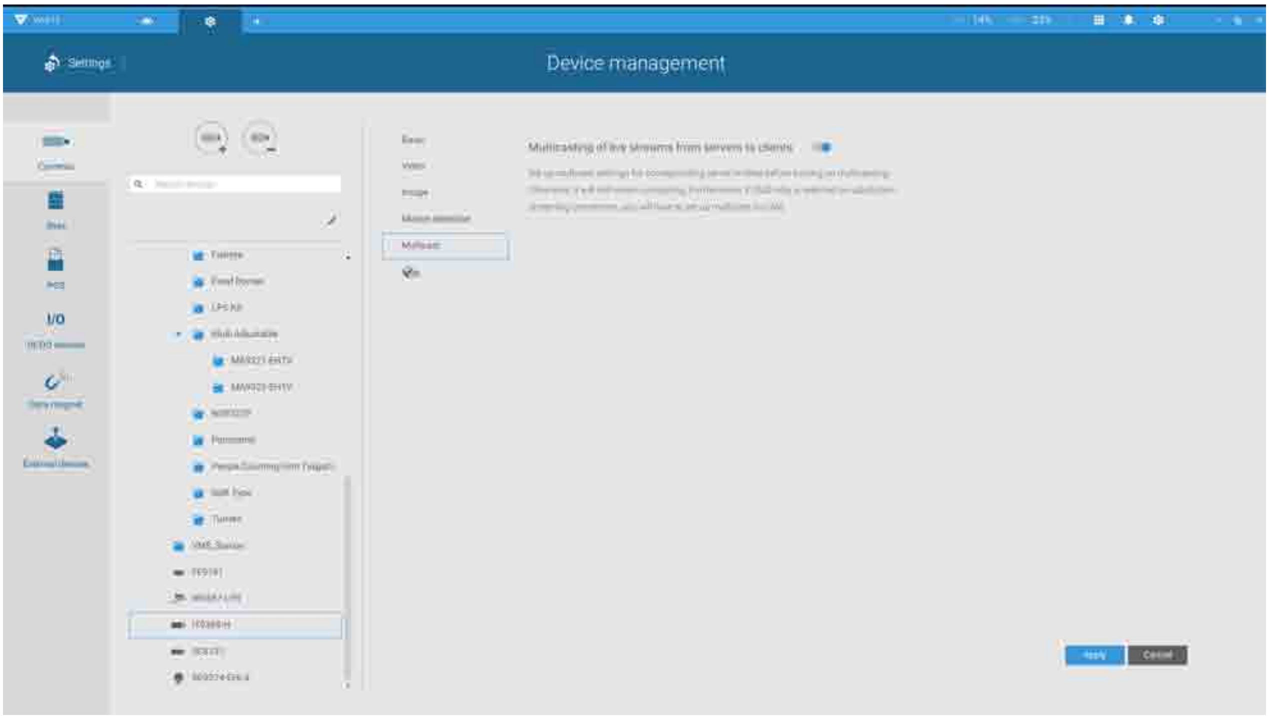
☑ Enable multicasting of live streams from server to clients

IP Address 239.128.11.99

Port 5000 ~ 20000

To enable Multicasting on a camera:

1. Enter Settings > Device > Cameras.
2. Single-click to select a camera for which you want to enable the Multicasting.
3. Click to select the Multicast tab.
4. Click the Multicasting slide button.
5. Click the **Apply** button.

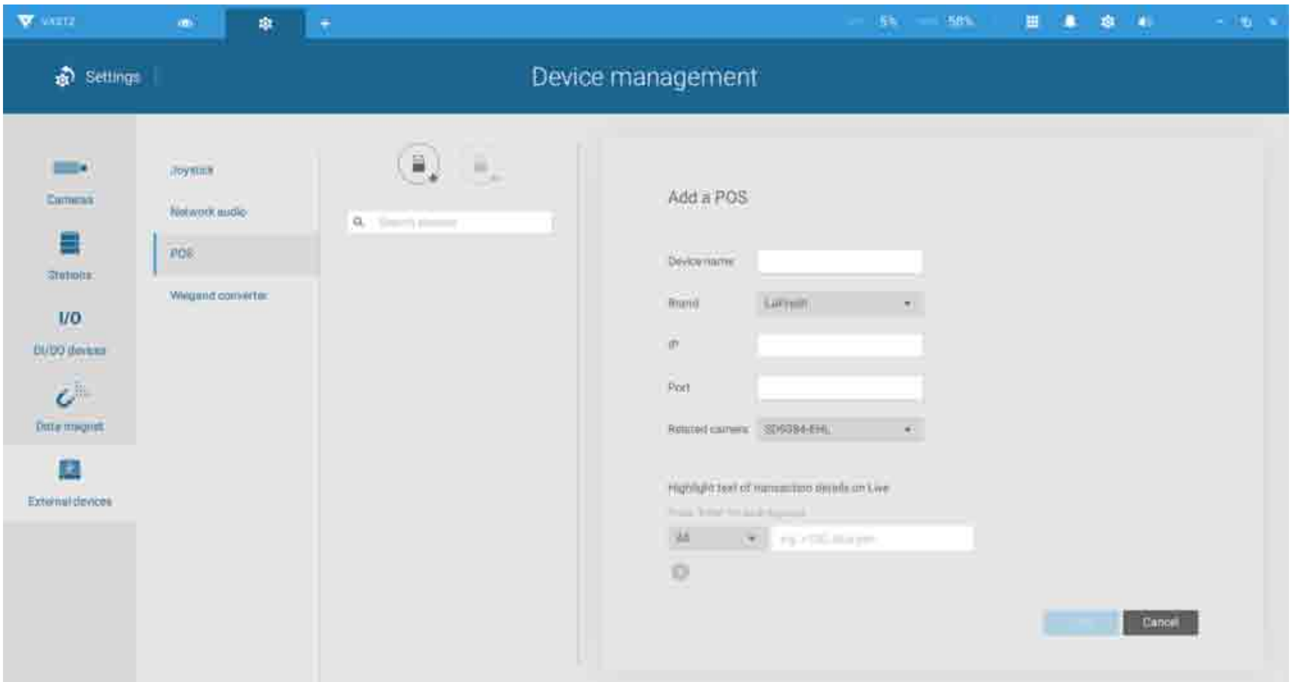


4-7. Settings > Device > External Devices > POS

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.



Add a POS

Device name

Brand Lafresh

IP

Port

Related camera SD9384-EHL

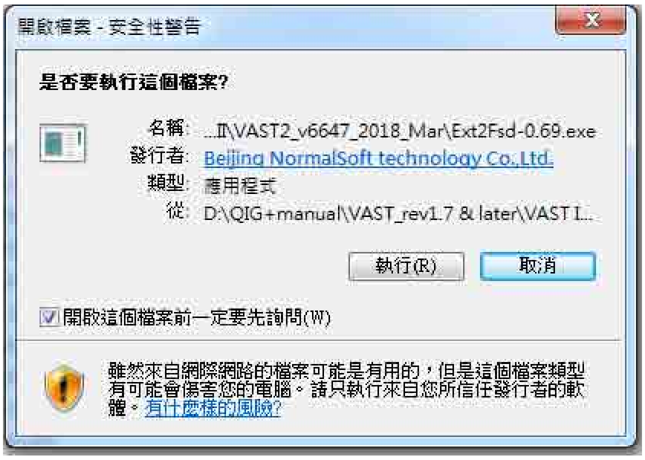
Highlight text of transaction details on Live

4-8. Settings > Device > Local DB

Since some of VIVOTEK's NVRs run 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.



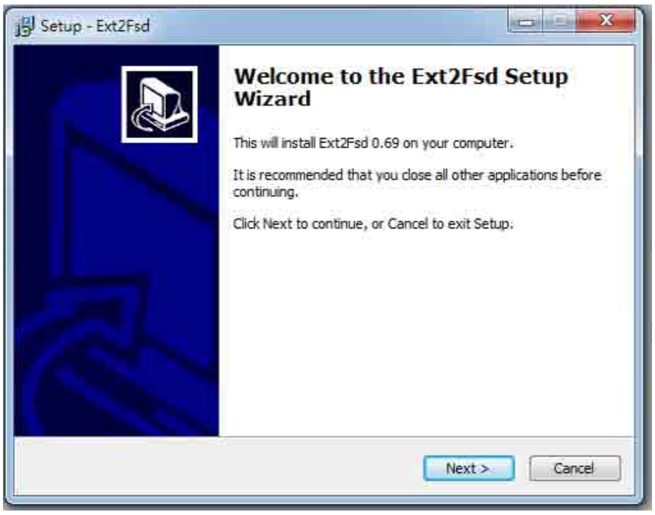
開啟檔案 - 安全性警告

是否要執行這個檔案?

名稱: ...I\VAST2_v6647_2018_Mar\Ext2Fsd-0.69.exe
發行者: Beijing NormalSoft technology Co.,Ltd.
類型: 應用程式
從: D:\QIG+manual\VAST_rev1.7 & later\VAST I...

☑ 開啟這個檔案前一定要先詢問(W)

雖然來自網際網路的檔案可能是有用的，但是這個檔案類型有可能會傷害您的電腦。請只執行來自您所信任發行者的軟體。有什麼樣的風險?



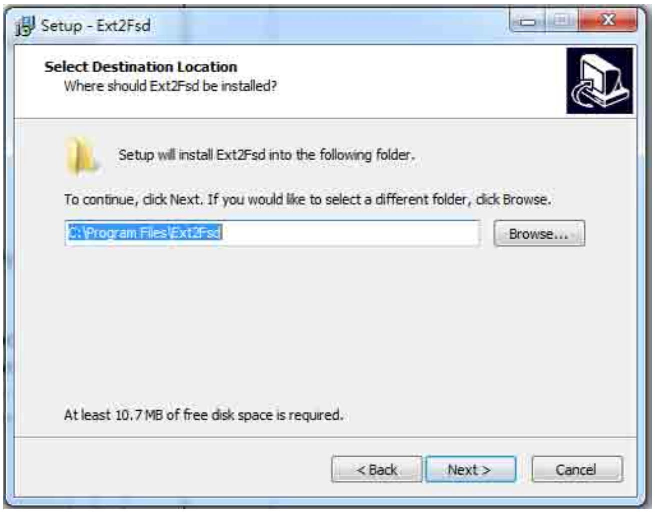
Setup - Ext2Fsd

Welcome to the Ext2Fsd Setup Wizard

This will install Ext2Fsd 0.69 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.



Setup - Ext2Fsd

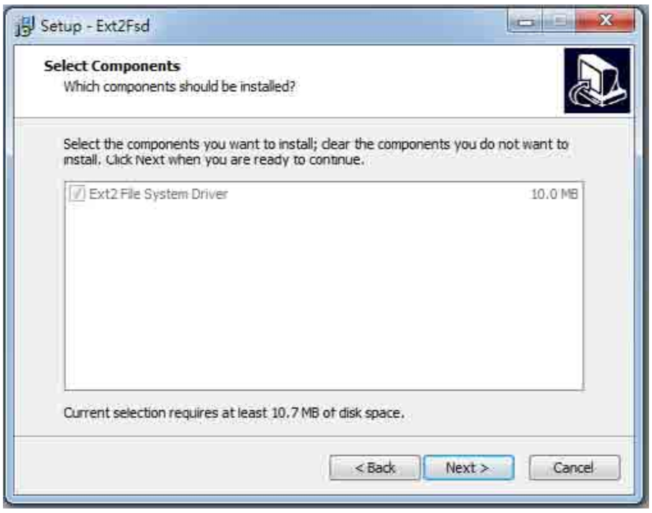
Select Destination Location
Where should Ext2Fsd be installed?

Setup will install Ext2Fsd into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Ext2Fsd

At least 10.7 MB of free disk space is required.



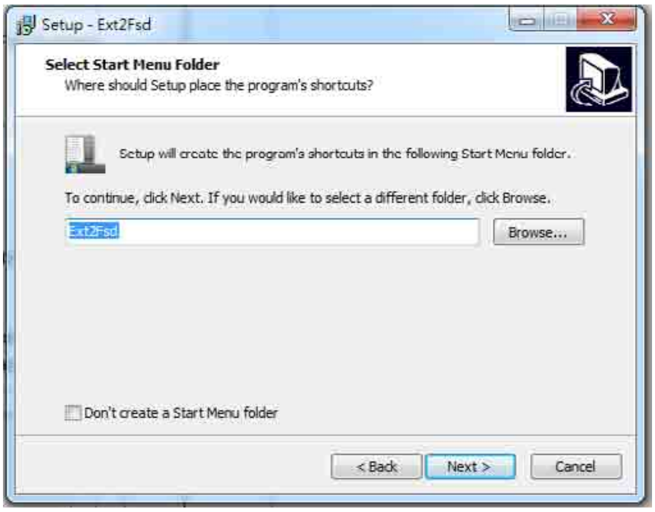
Setup - Ext2Fsd

Select Components
Which components should be installed?

Select the components you want to install; clear the components you do not want to install. Click Next when you are ready to continue.

☑ Ext2 File System Driver 10.0 MB

Current selection requires at least 10.7 MB of disk space.



Select Start Menu Folder

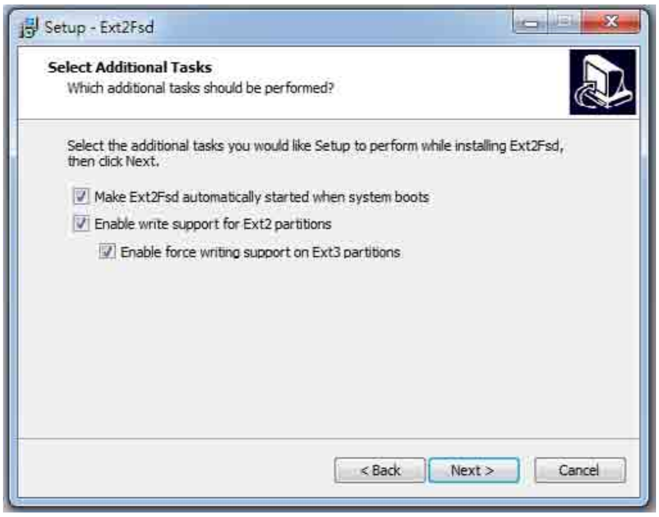
Where should Setup place the program's shortcuts?

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

□ Don't create a Start Menu folder



Select Additional Tasks

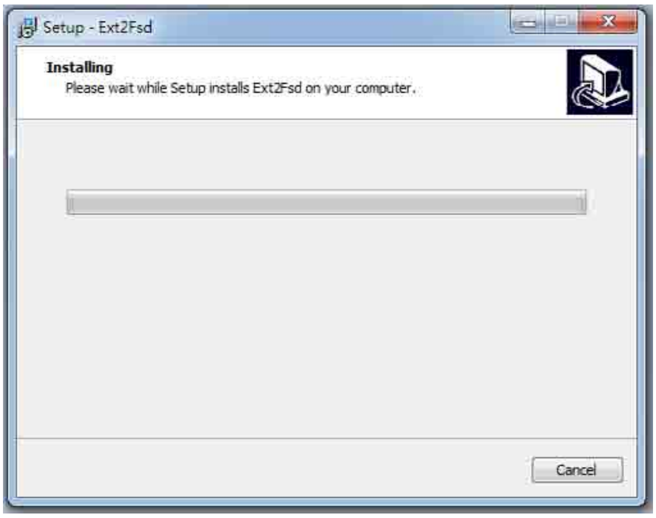
Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing Ext2Fsd, then click Next.

☑ Make Ext2Fsd automatically started when system boots

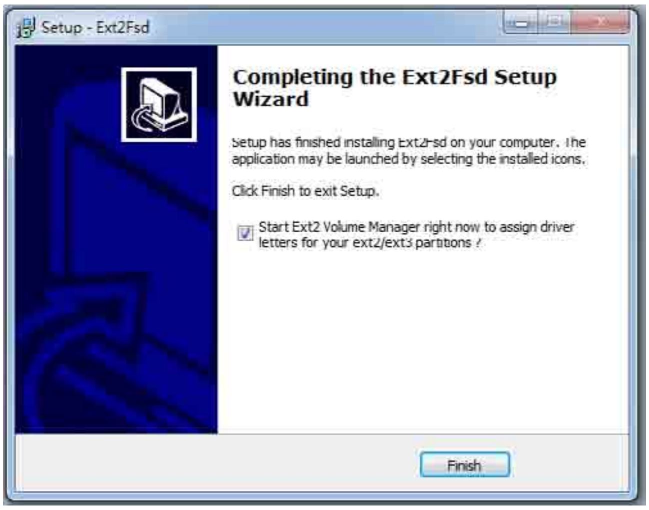
☑ Enable write support for Ext2 partitions

☑ Enable force writing support on Ext3 partitions



Installing

Please wait while Setup installs Ext2Fsd on your computer.

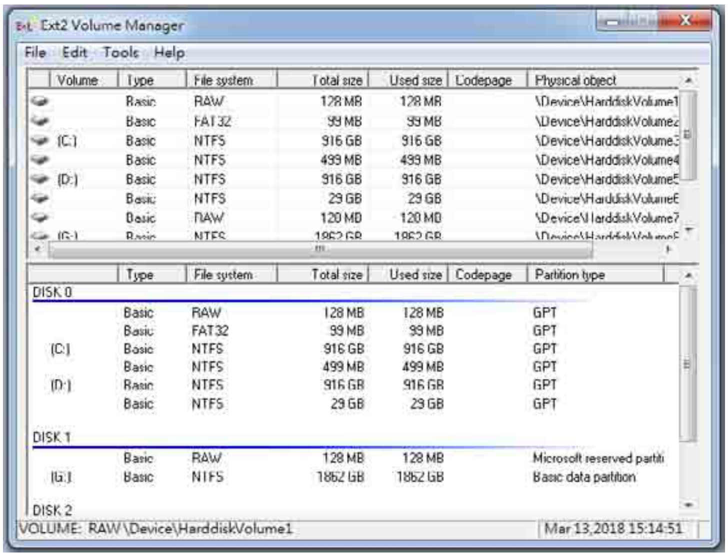


Completing the Ext2Fsd Setup Wizard

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 ?

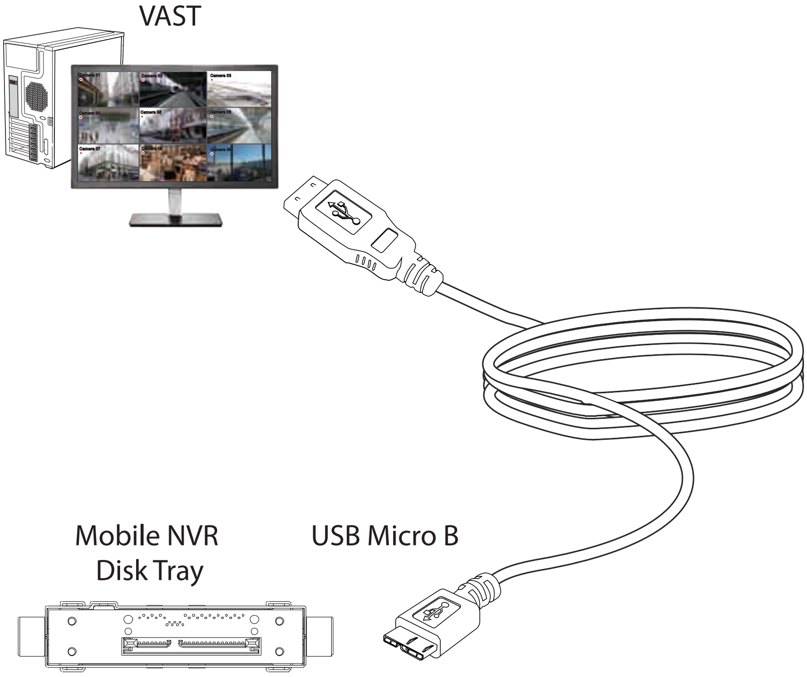


Volume	Type	File system	Total size	Used size	Codepage	Physical object
	Basic	RAW	128 MB	128 MB		\Device\HarddiskVolume1
	Basic	FAT32	99 MB	99 MB		\Device\HarddiskVolume2
(C:)	Basic	NTFS	916 GB	916 GB		\Device\HarddiskVolume3
	Basic	NTFS	499 MB	499 MB		\Device\HarddiskVolume4
(D:)	Basic	NTFS	916 GB	916 GB		\Device\HarddiskVolume5
	Basic	NTFS	29 GB	29 GB		\Device\HarddiskVolume6
	Basic	RAW	120 MB	120 MB		\Device\HarddiskVolume7
(G:)	Basic	NTFS	1862 GB	1862 GB		\Device\HarddiskVolume

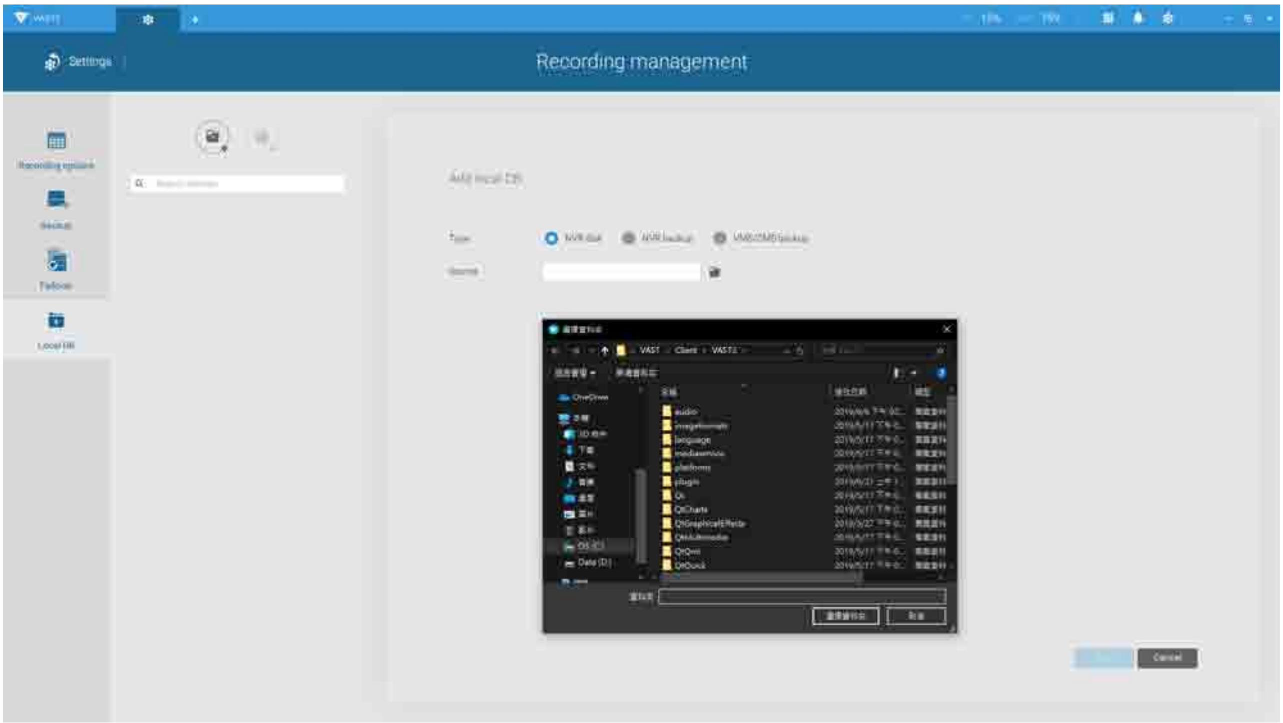
	Type	File system	Total size	Used size	Codepage	Partition type
DISK 0						
	Basic	RAW	128 MB	128 MB		GPT
	Basic	FAT32	99 MB	99 MB		GPT
(C:)	Basic	NTFS	916 GB	916 GB		GPT
	Basic	NTFS	499 MB	499 MB		GPT
(D:)	Basic	NTFS	916 GB	916 GB		GPT
	Basic	NTFS	29 GB	29 GB		GPT
DISK 1						
	Basic	RAW	128 MB	128 MB		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.

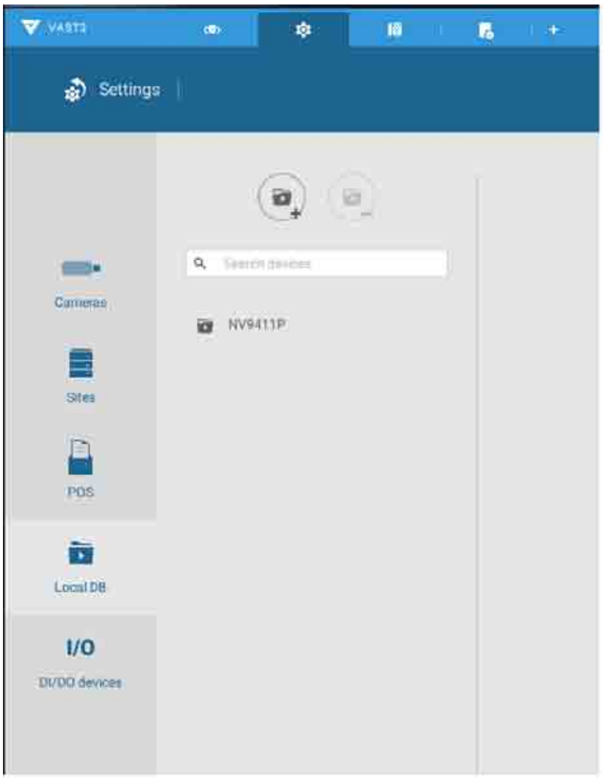


3. From VAST, enter **Settings** > **Device** > **Locabl DB**.
4. There are 3 import types:
    1. **NVR disk**: the drive tray box removed from a mobile NVR.
    2. **NVR backup**: the recorded videos exported from an NVR using a USB thumb disk or portable drive.
    3. **VAST backup**: scheduled backup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

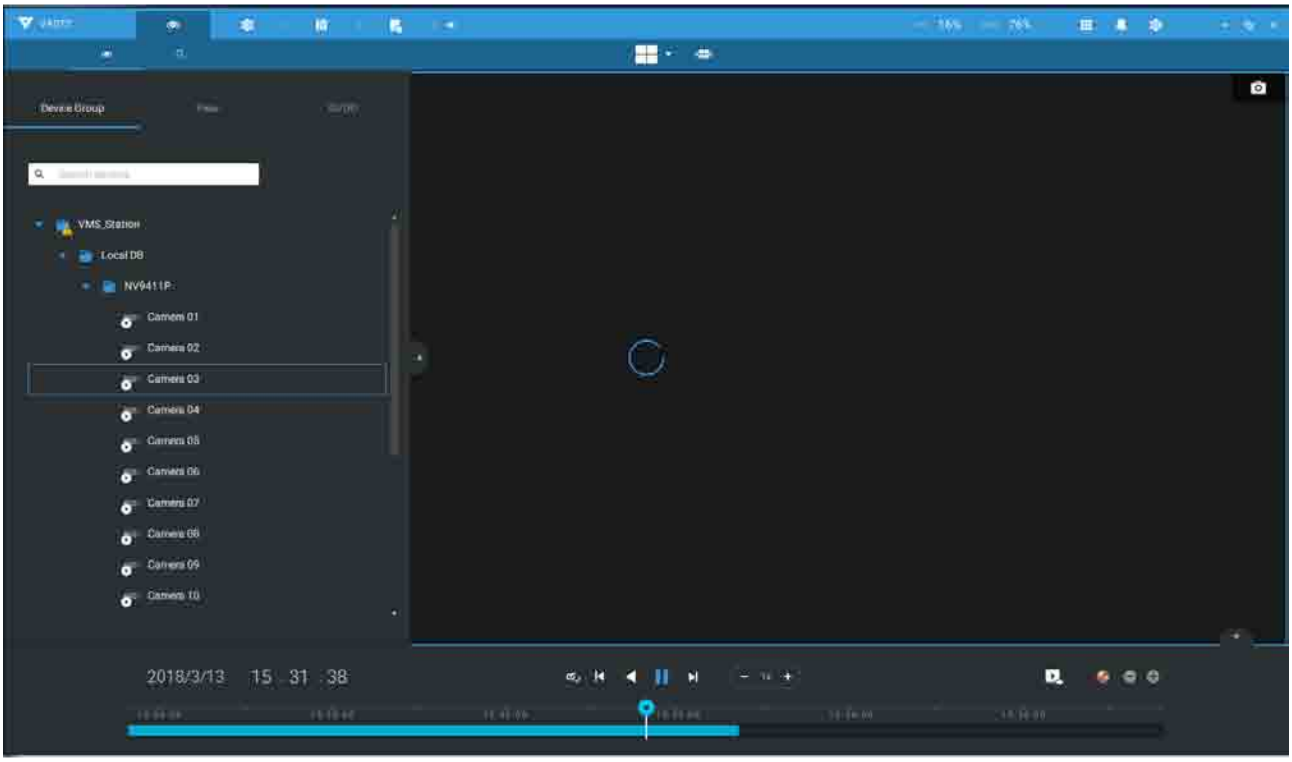


5. Taking a mobile NVR's disk drive as an example, click the 📁 Source select button to locate the disk drive.

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 SMTP. Click on the Add SMTP button.
Enter your mail server's domain name or IP address. Enter credentials for access to the mail service.
If SSL encrypted transmission is preferred, select its checkbox.

Click Add to complete the configuration.

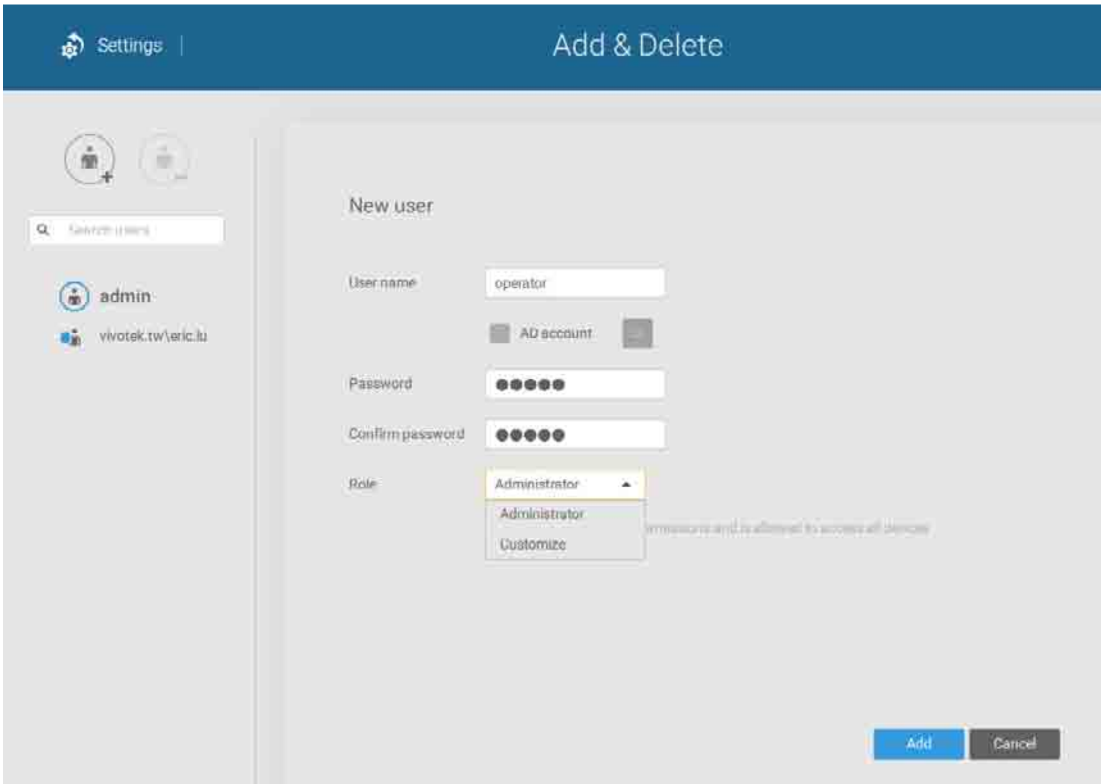
4-10. Settings > IO Box and Related Configuration

Please refer to page 131 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.



New user

User name: operator

□ AD account

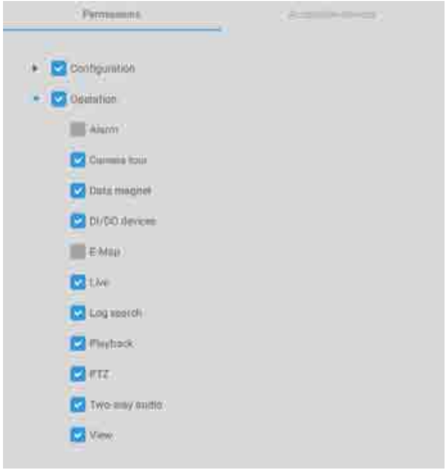
Password: ●●●●●

Confirm password: ●●●●●

Role: Administrator
- Administrator
- Customize

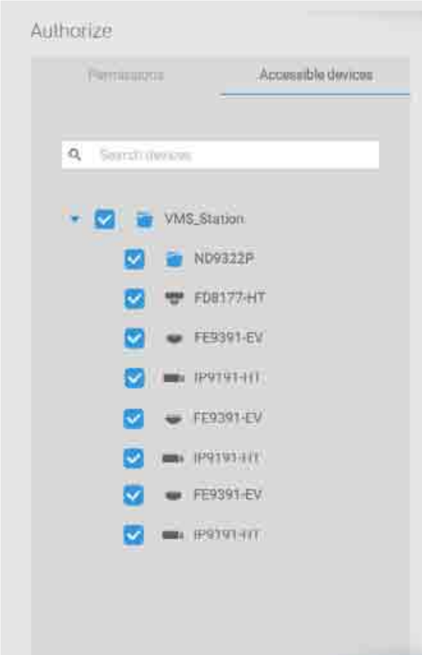
Use the Customize option to limit the authorized actions of a user.

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.



- ▶ ☑ Configuration
- ▼ ☑ Operation
  - □ Alarm
  - ☑ Camera tour
  - ☑ Data magnet
  - ☑ DI/DO devices
  - □ E-Map
  - ☑ Live
  - ☑ Log search
  - ☑ Playback
  - ☑ PTZ
  - ☑ Two-way audio
  - ☑ View

In the Accessible devices tab, click to select the cameras that a user can access. Some users may only need to access specific devices.



Authorize

Permissions | Accessible devices

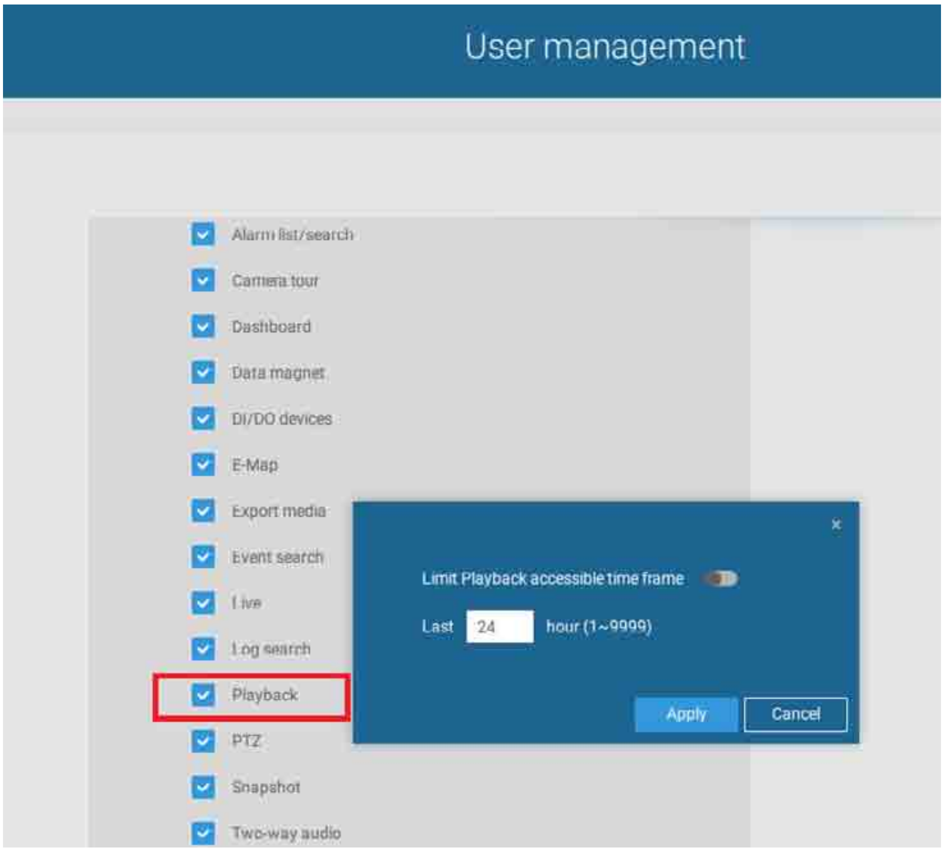
Search devices

- ☑ VMS_Station
  - ☑ ND9322P
  - ☑ FD8177-HT
  - ☑ FE9391-EV
  - ☑ IP9191-HT
  - ☑ FE9391-EV
  - ☑ IP9191-HT
  - ☑ FE9391-EV
  - ☑ IP9191-HT

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.

Note that you can place a limitation on a user's access right to the recorded videos by setting a barrier for access to the older recordings. Recordings older than a configurable period of time will not be accessible.



User management

- ☑ Alarm list/search
- ☑ Camera tour
- ☑ Dashboard
- ☑ Data magnet
- ☑ DI/DO devices
- ☑ E-Map
- ☑ Export media
- ☑ Event search
- ☑ Live
- ☑ Log search
- ☑ Playback
- ☑ PTZ
- ☑ Snapshot
- ☑ Two-way audio

Limit Playback accessible time frame

Last 24 hour (1~9999)

Add a New User Account - Windows AD Account

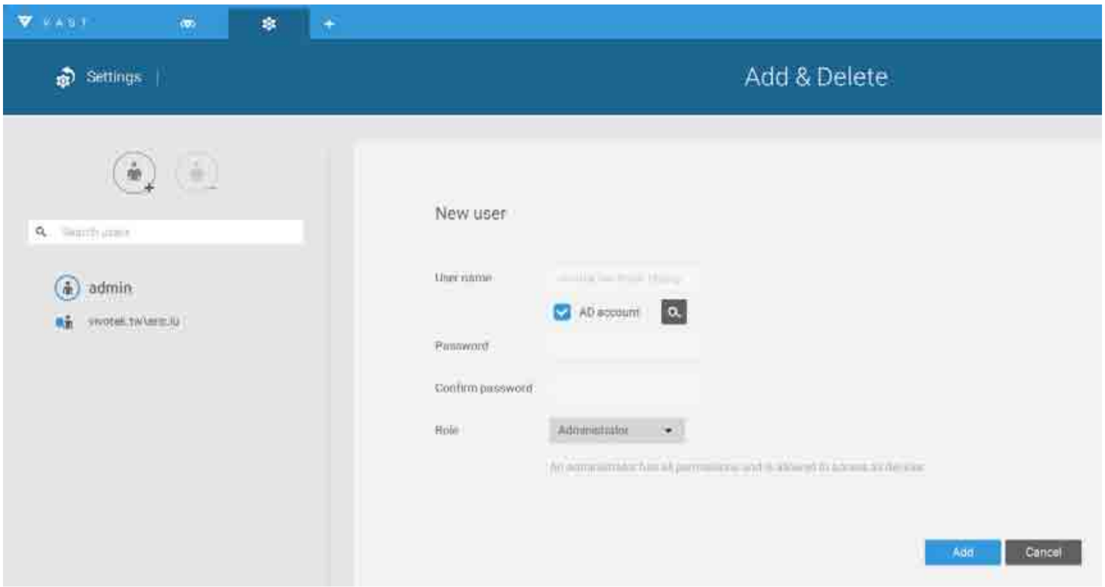
In an established, enterprise network environment, the support for Windows AD (Active Directory) infrastructure enables ease of integration using the credentials of existing users. Using the same AD authentication methodologies, you can configure the clients or users in an established network to access 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.



New user

User name

☑ AD account

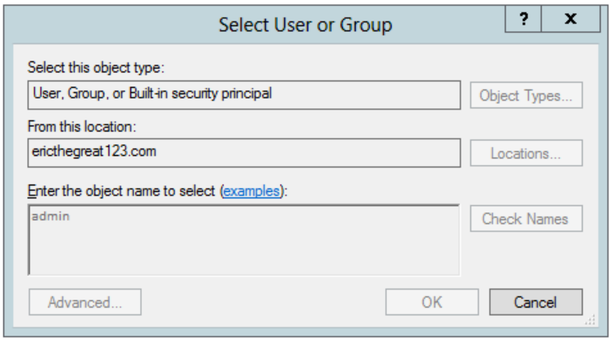
Password

Confirm password

Role: Administrator

2. Click the Search 🔍 button.

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



Select this object type:

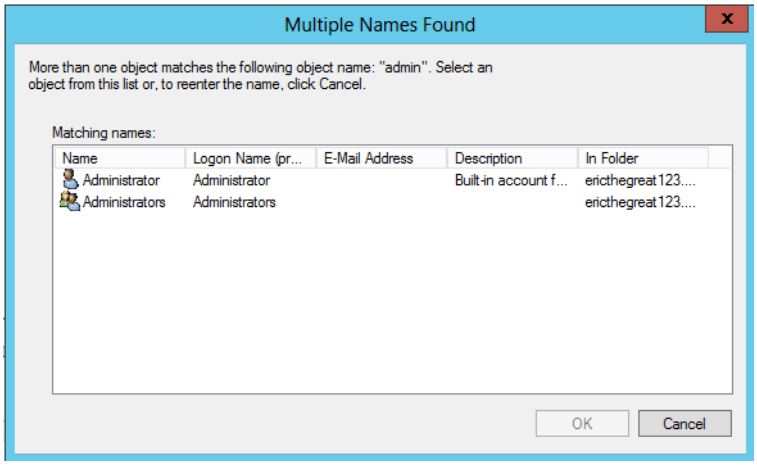
User, Group, or Built-in security principal

From this location:

ericthegreat123.com

Enter the object name to select (examples):

admin



More than one object matches the following object name: "admin". Select an object from this list or, to reenter the name, click Cancel.

Matching names:

Name	Logon Name (pr...	E-Mail Address	Description	In Folder
Administrator	Administrator		Built-in account f...	ericthegreat123....
Administrators	Administrators			ericthegreat123....

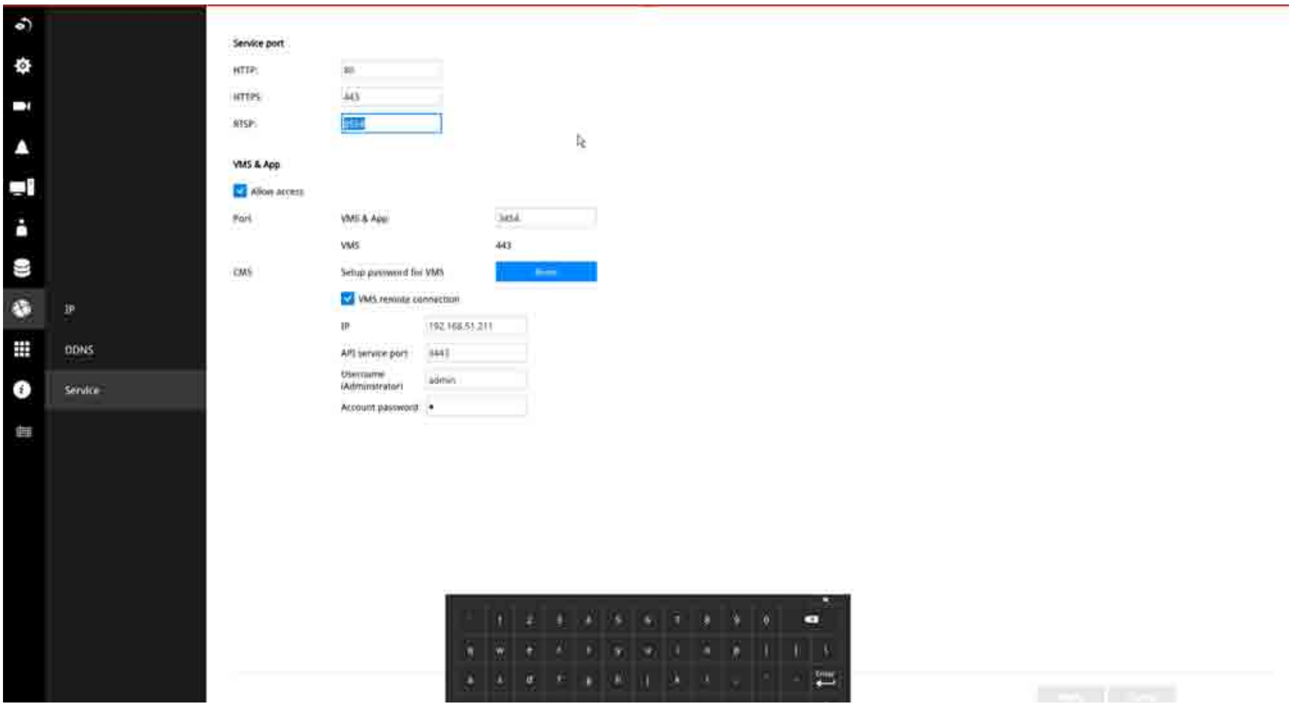
4. Enter the password twice for the AD user.

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

4-12. Settings > VIVOCloud

If users have an existing VIVOCloud account, they can join their current configuration with VAST2, such as an NVR and the cameras managed by it.

The precondition is, you must allow the NVR to be accessed from a VAST server. Open a console to the NVR, and enter IP > Service, to click on Allow access.



Service port

HTTP: 80

HTTPS: 443

RTSP: [illegible]

VMS & App

☑ Allow access

Port — VMS & App: 3454

VMS: 443

CMS — Setup password for VMS

☑ VMS remote connection

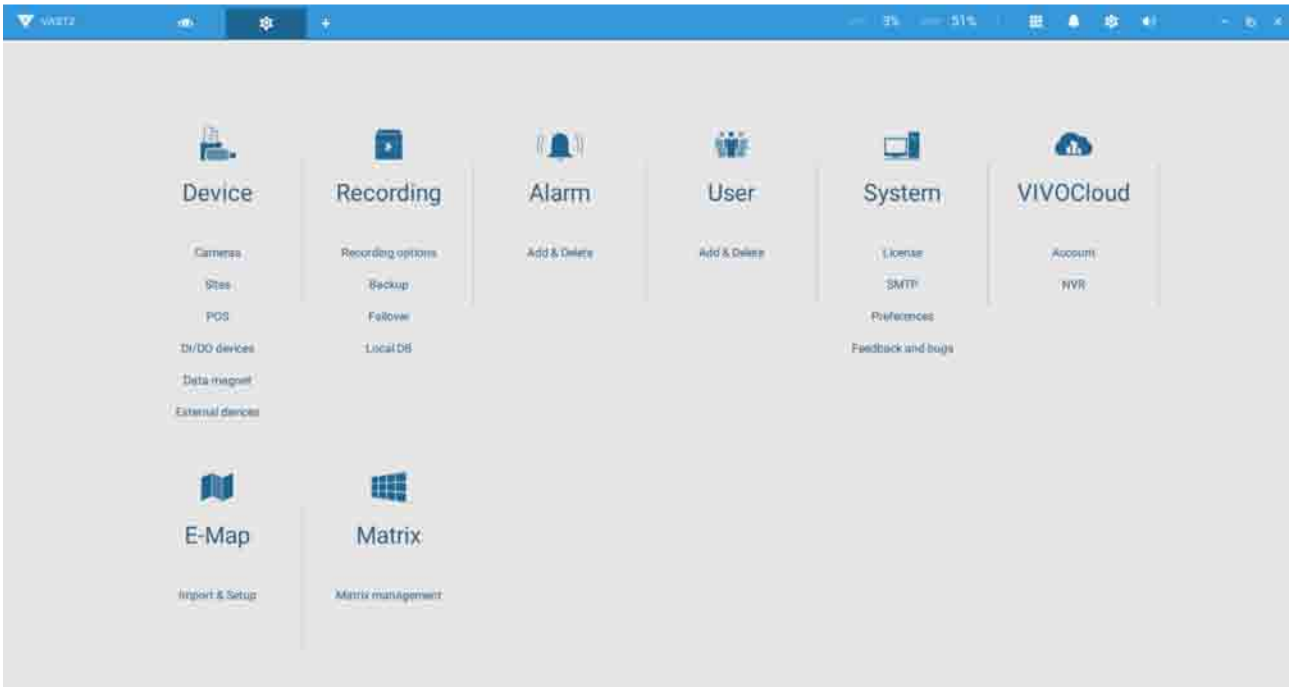
IP: 192.168.51.211

API service port: 8443

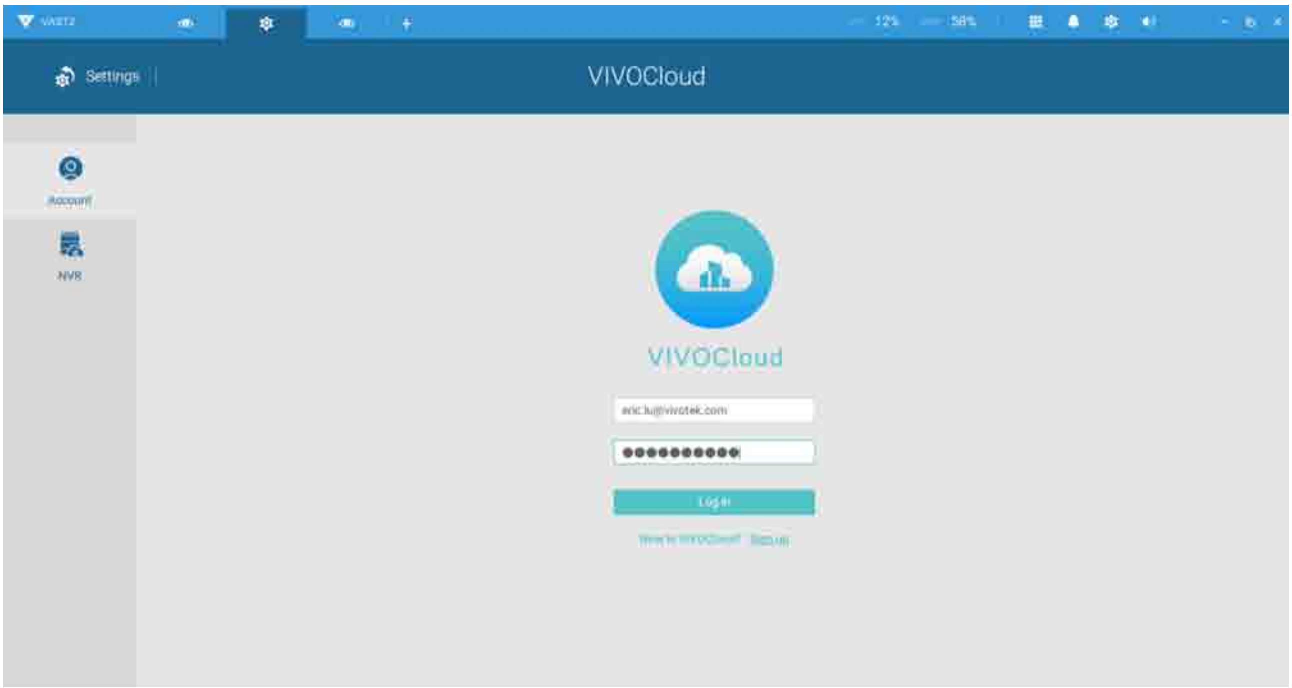
Username (Administrator): admin

Account password: •

On the VAST client, click Settings > VIVOCloud.



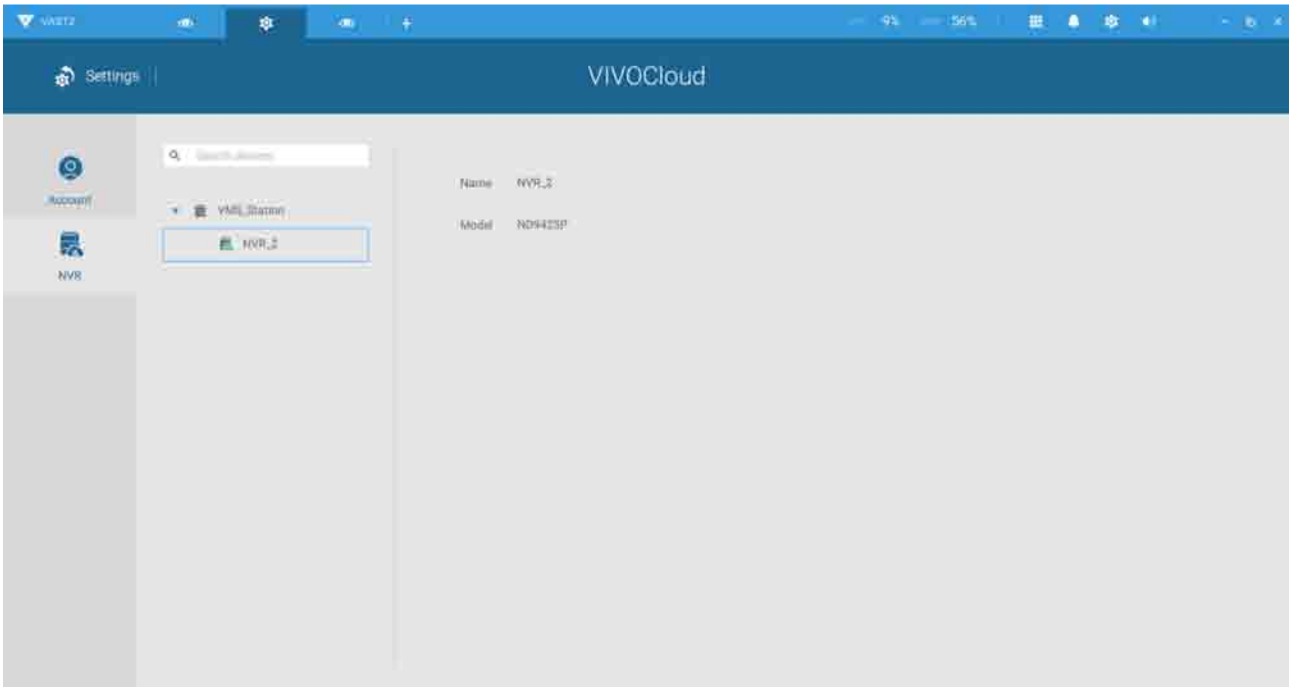
Log in using your VIVOCloud credentials.



eric.lu@vivotek.com

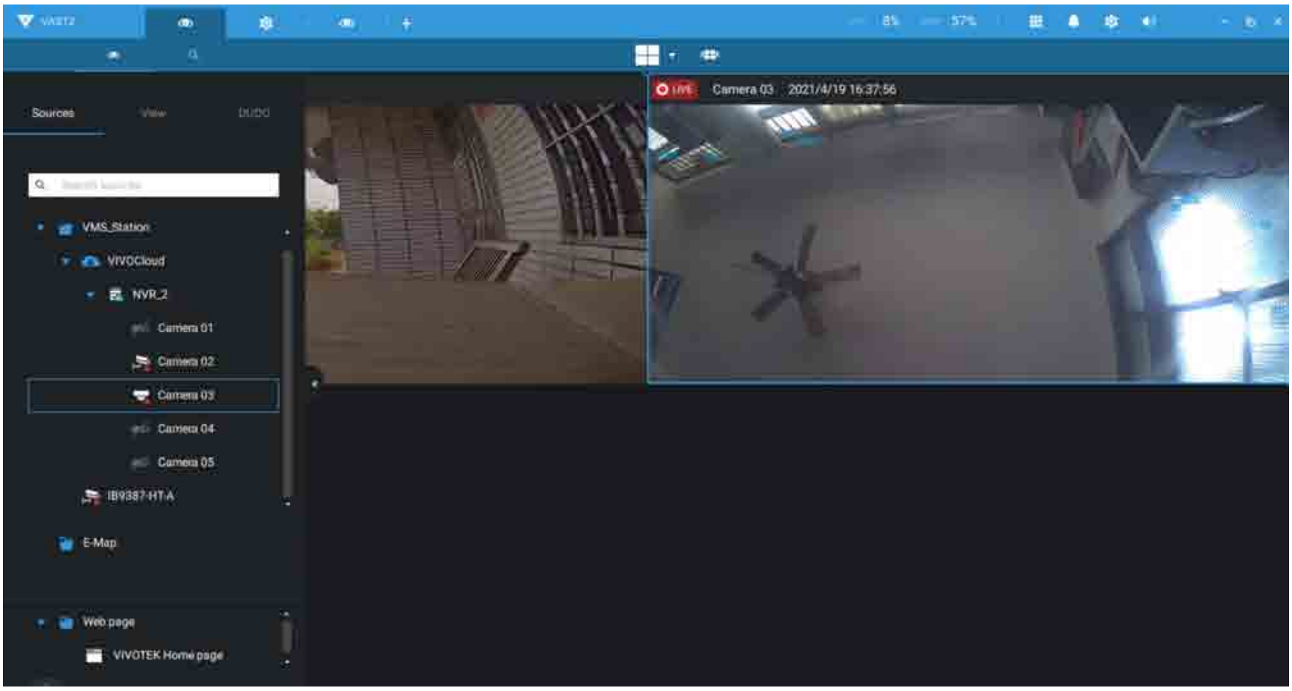
●●●●●●●●●●●

The NVR will be listed under the VIVOCloud device tree.



Name NVR_2

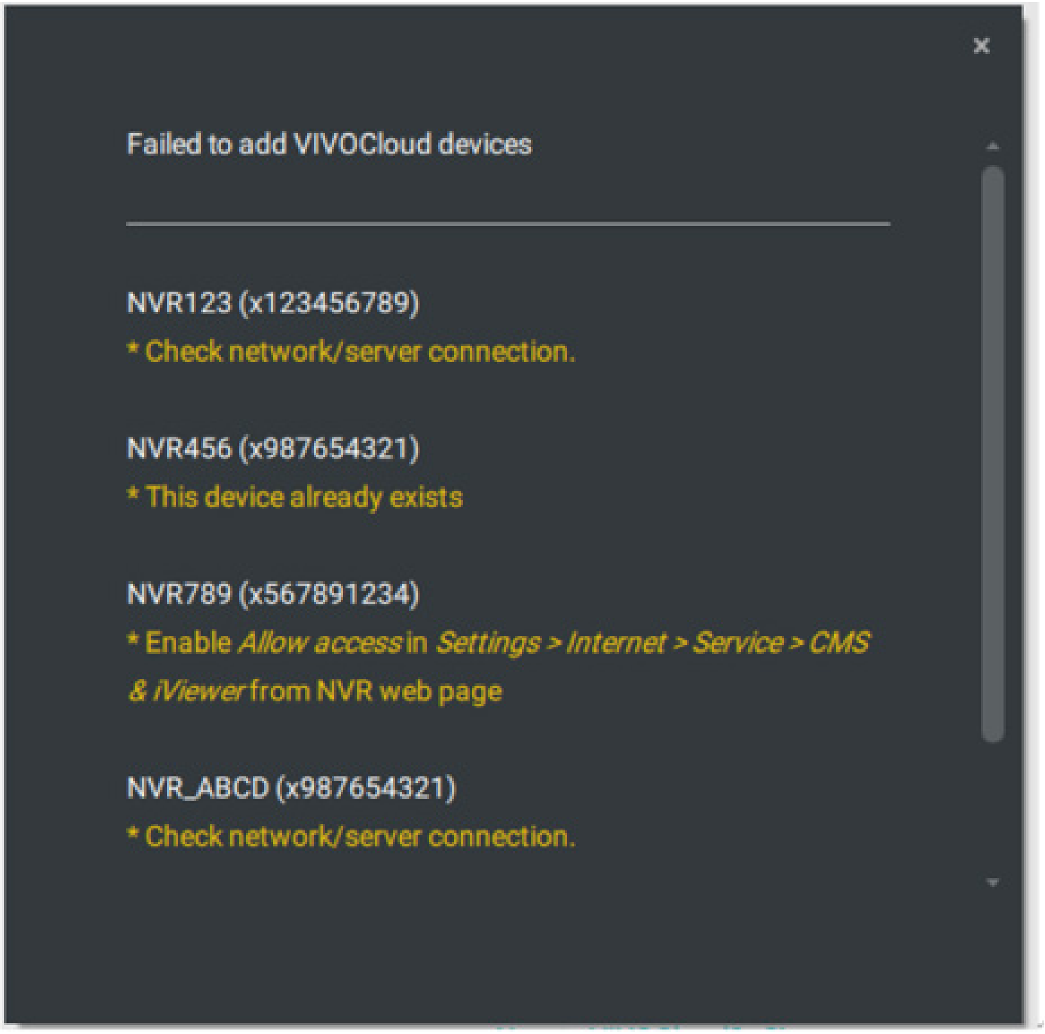
Model ND9425P



Camera 03 2021/4/19 16:37:56

If the NVR managed through the VIVOCloud is connected via a local or P2P network, the connection should be normal. If the NVR is connected through VIVOCloud Relay, a 28 minutes timeout will be imposed, and you can use the connect button to re-connect.

You can encounter this message with connection problems or you did not allow the access from a VAST server. You have to log out your VIVOCloud account and log in again after you solve the above problems.



Failed to add VIVOCloud devices

NVR123 (x123456789)

* Check network/server connection.

NVR456 (x987654321)

* This device already exists

NVR789 (x567891234)

* Enable *Allow access* in *Settings > Internet > Service > CMS & iViewer* from NVR web page

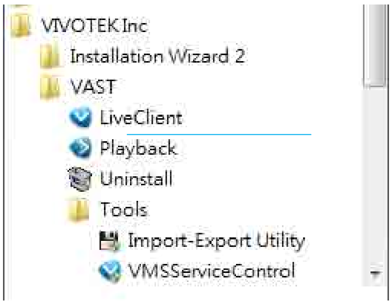
NVR_ABCD (x987654321)

* Check network/server connection.

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.

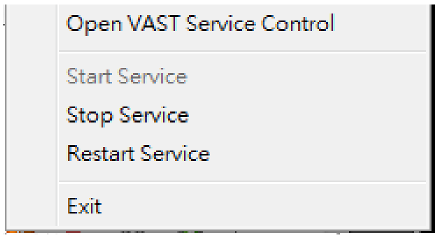
Under Microsoft Windows, choose "**Start > All Programs > VIVOTEK Inc > VAST > Tools > VMServiceControl.**"

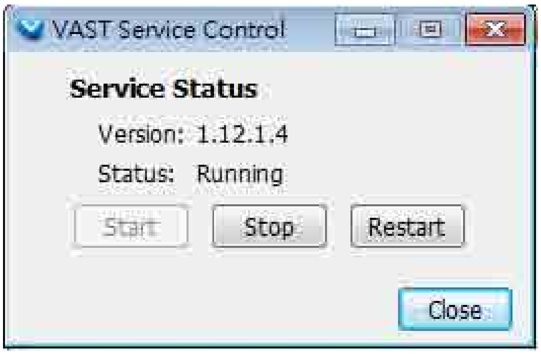


You may also find it in the system tray icon of the tool bar, which indicates that the service is running:

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:





Service Status

Version: 1.12.1.4

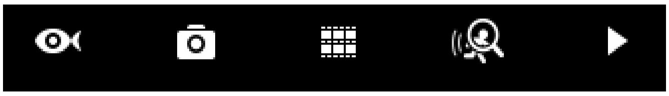
Status: Running

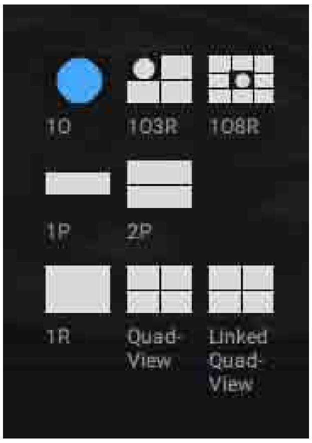
Here you can manually start, stop and restart the service.

Appendix B: Fisheye Camera Dewarp Modes

By default, a circular view is displayed when a fisheye camera is successfully connected. To display Regional, Panoramic, or the combination of different views,

1. Mouse over the view cell of a fisheye camera.
2. The onscreen control panel will appear. Click on the Fisheye button.
3. The Dewarp mode pane will prompt. Select a dewarp mode.





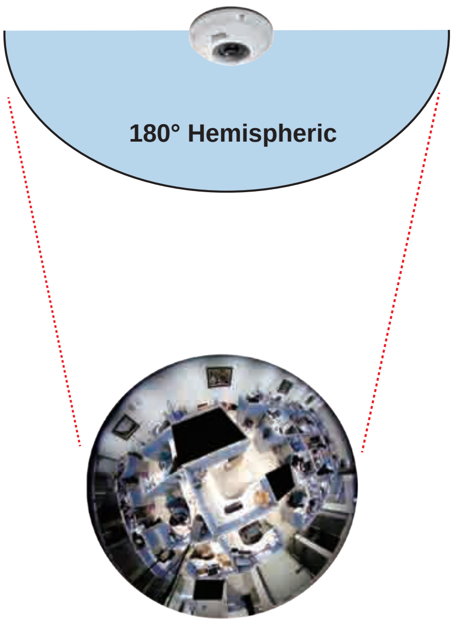
The display modes available are: 1O (Original), 1P (Panoramic), 1R (Regional), 2P (2 Panoramic), 1O3R (1 Original & 3 Regional), 4R (Quad Regional), 1O8R (1 Original & 8 Regional), and 4R Pro (4 Proactive) modes.

Fisheye Display Modes: below are conceptual drawings for different display modes.

1O (Single Original) Display mode:

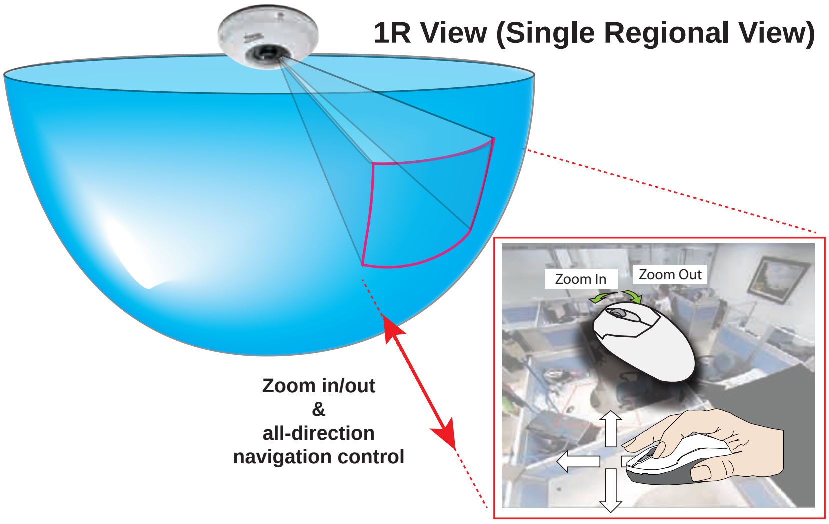
An **Original** oval view covers the hemisphere taken by the fisheye lens.

1O View (Original View)



1R (Single Regional) Display mode:

A **Regional** view crops a portion of the hemisphere as a region of interest. You can zoom in or out or move the view area elsewhere from on the regional view.


1R View (Single Regional View)

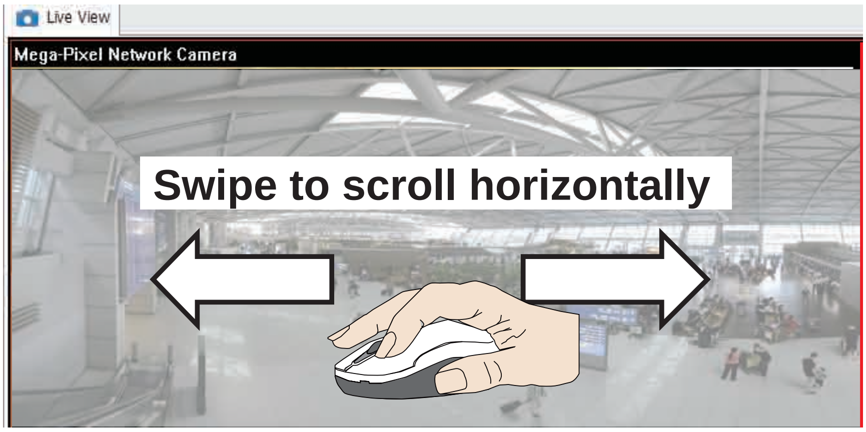
A Regional view is dewarped, by correcting images from the distorted oval view to a rectangular and visually proportional image.

1P (Single **Panoramic**) Display mode:

With image correction algorithms in firmware, the hemispheric image is transformed into a rectilinear stripe in the 1P display mode. Viewers can use the PTZ panel or simply use mouse control to quickly move through the 360º panoramic view.

Note that the 1P view is apt for an overview, the Zoom in/out function does not apply in this mode.

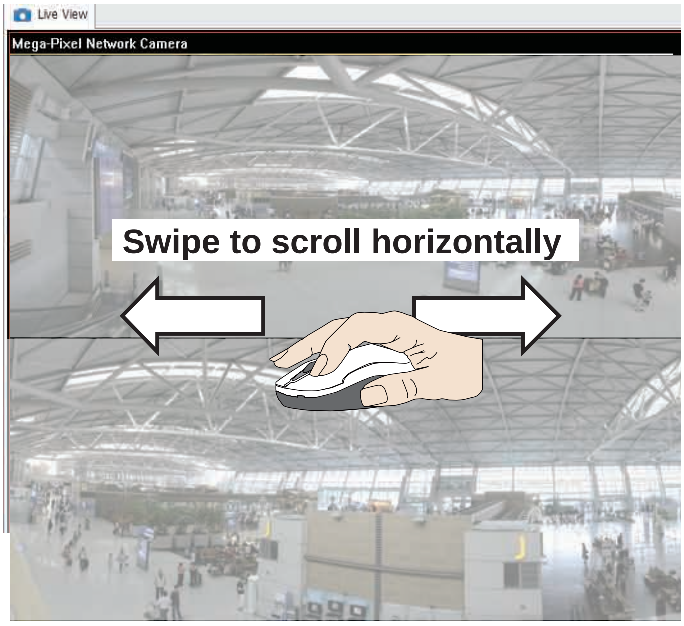
1P (Panoramic) Mode Screen Control



2P (2 Panoramic) Display mode:

Two dewarped rectangular views are placed one on top of another each showing 180 degree of panoramic view. The 2P view looks like the upper view shows the front of hemisphere, and the lower view the rear half of the hemisphere.

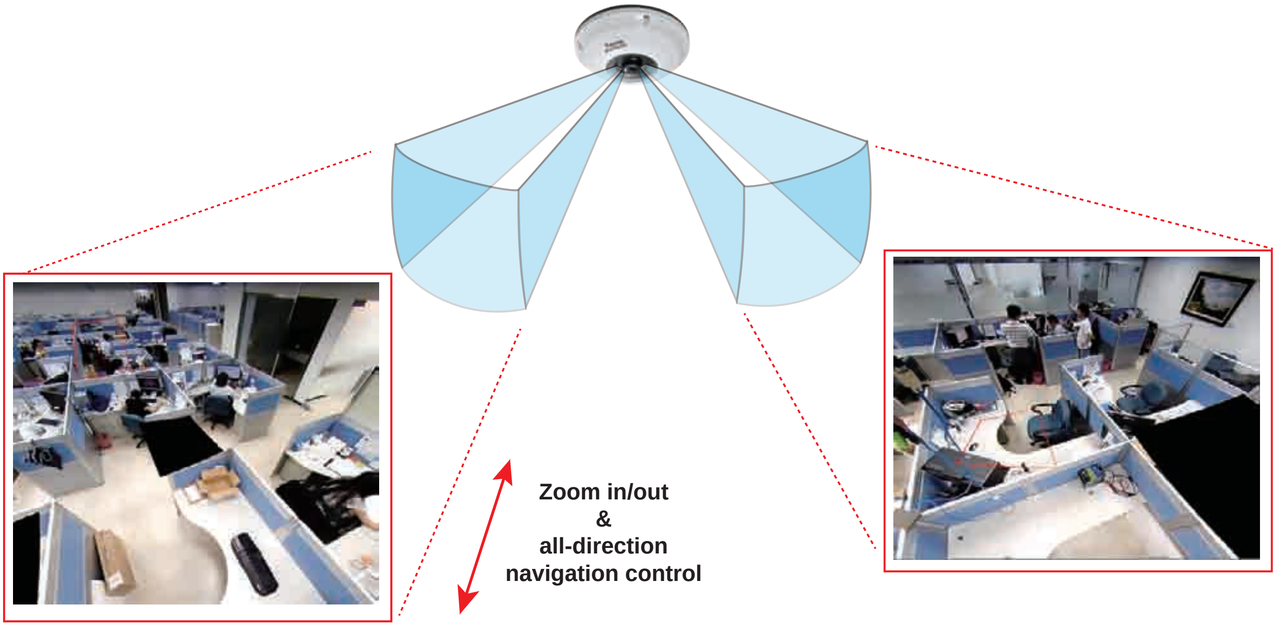
2P (Panoramic) Mode Screen Control



1O3R (One Original & 3 Regional) Display mode:

Fisheye cameras also support the display of multiple regional views taken from within the same hemisphere, and they can be displayed with or without an Original view in its view cell.

3R View (Regional View)



* Only two regional views are shown for simplicity reason

NOTE:

The various display modes require the support of D3D technologies by your display card on the LiveClient or Playback station. Most off-the-shelf display cards today support this feature.

The onscreen mouse control is very agile. Therefore, use the PTZ panel for more delicate moves in a field of view. **Pan** and **Patrol** moves are also supported if you have configured preset PTZ positions in the camera's firmware. Note that the Pan move takes place in the Panoramic and Regional views, while the Patrol function through preset positions applies only in the Regional views.

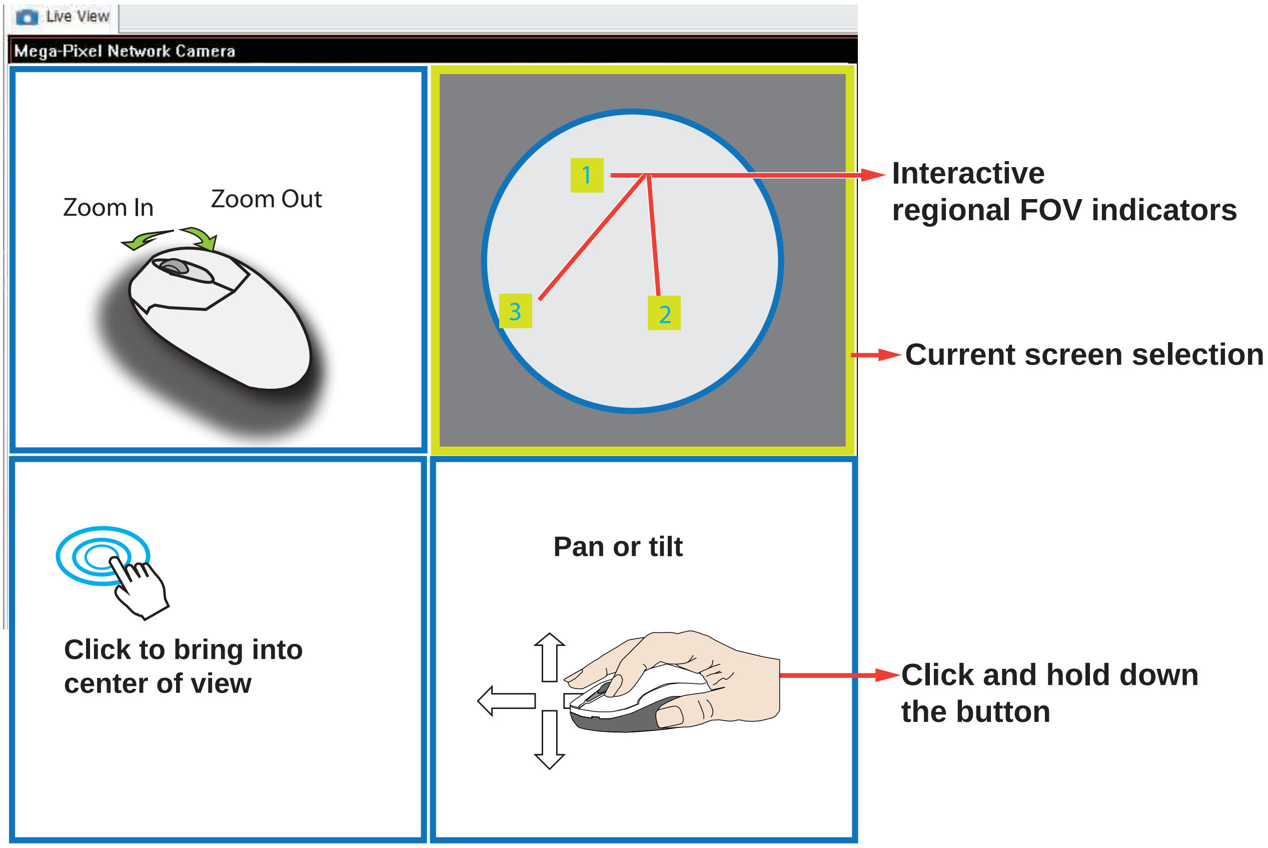
PTZ Mouse Control

The "Mount type" setting also determines the display modes available to your display modes. Please refer to fisheye camera's User Manual for more information.

A highly versatile mouse control is implemented with fisheye cameras. The same control takes effect on a browser management session, on the LiveClient utility, and even on a video playback screen. See the drawing below for how it works.

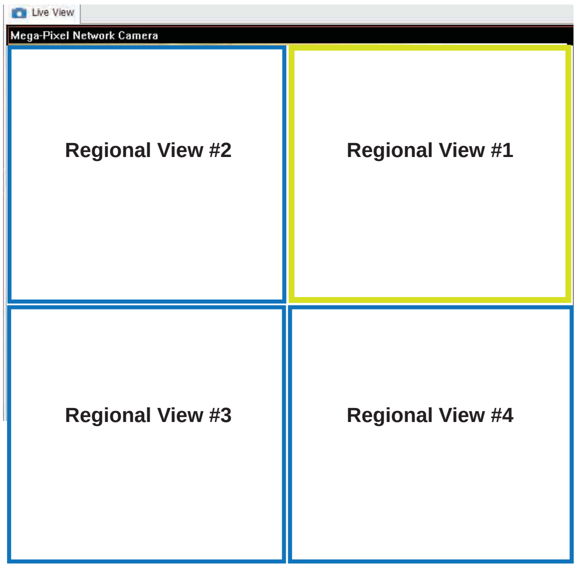
You can click and hold down the left mouse button to quickly swipe through the field of view, change the view angle, or use the mouse wheel to zoom in/out on a region of interest. However, the PTZ mouse control is only available in the **"R" (Regional) mode**. In the **Panoramic mode**, you can only scroll horizontally across the 180º or 360º panoramic view.

1O3R (Original & Regional) Mode Screen Control

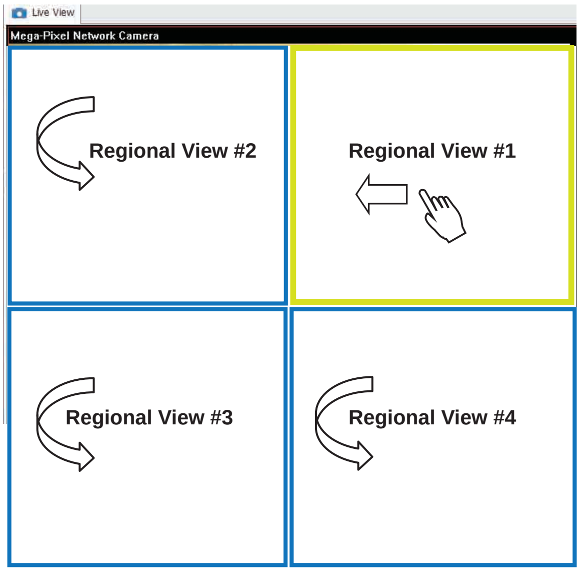

Live View
Mega-Pixel Network Camera
Zoom In
Zoom Out
1
2
3
Interactive regional FOV indicators
Current screen selection
Click to bring into center of view
Pan or tilt
Click and hold down the button

Below are the conceptual drawings for the other display modes. The available display modes can differ with different mount types:
Regular: 1O, 1P, 1R, 1O3R, 4R.
Wall mount: 1P2R, 1P3R.
For more information, you can refer to fisheye camera's user documents.

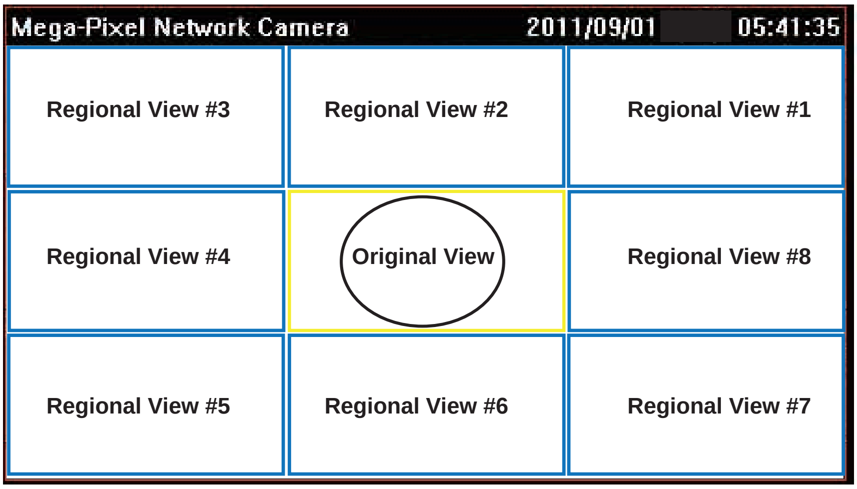
4R (Quad Regional) Display mode:



4RPro (4 Regional Proactive) Display mode:



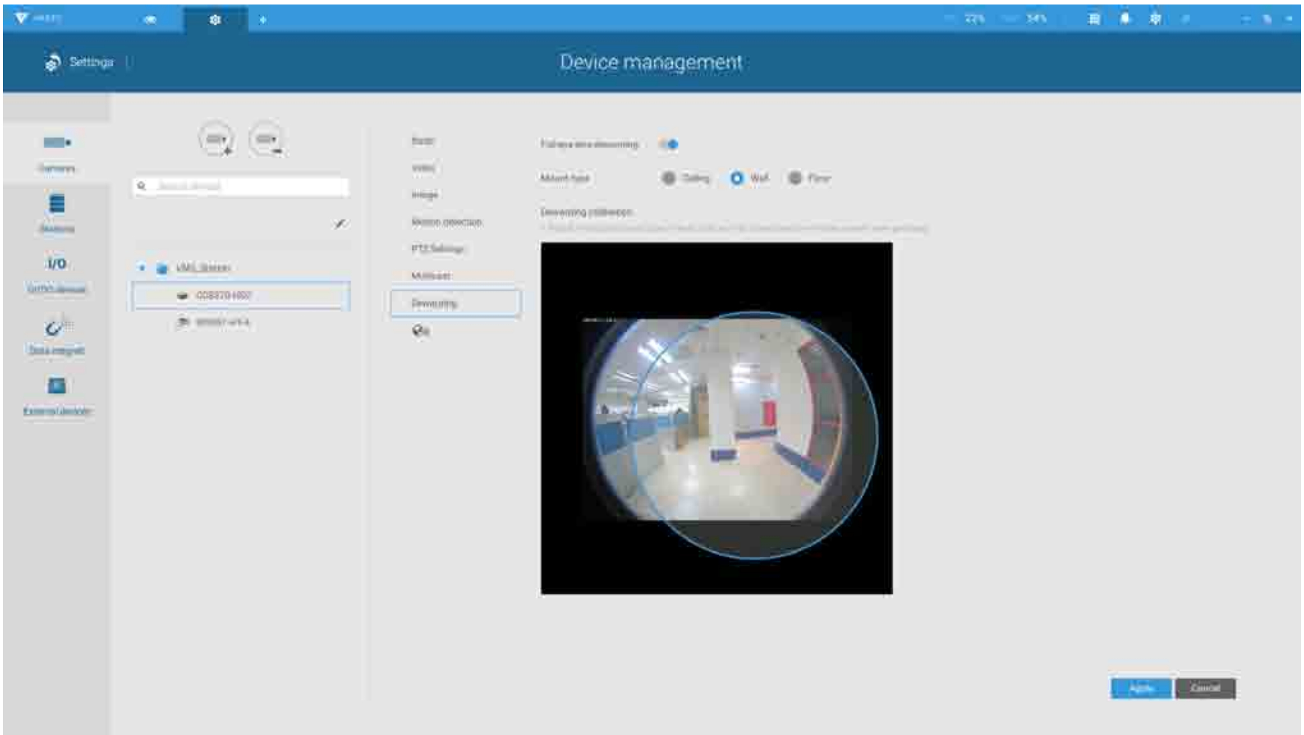
1O8R (One Original & 8 Regional) Display mode:

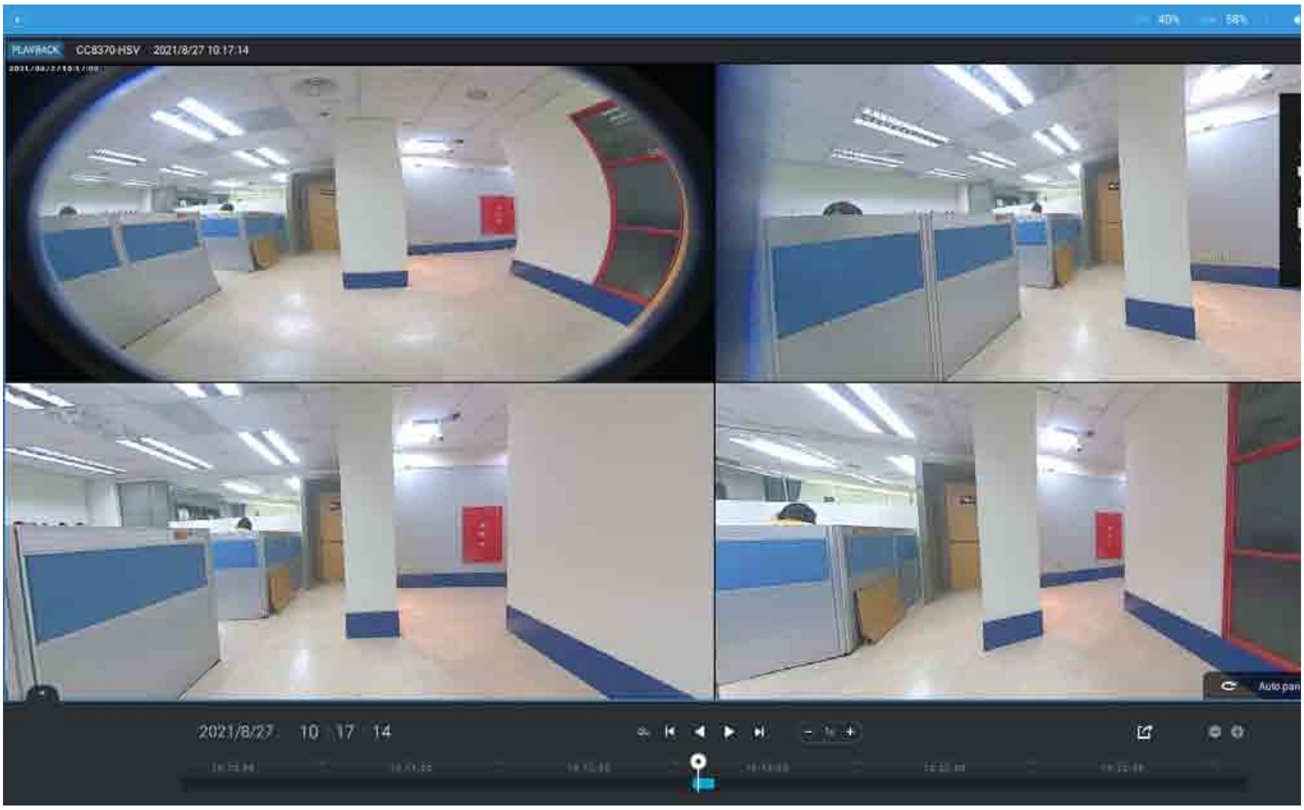


3rd-party Fisheye Dewarp

Via manual calibration, users can utilize dewarp functions for 3rd-party fisheye cameras through the Enable fisheye lens dewarping, and select a mount type. You can then align the blue cirlce with the fisheye's circular view.

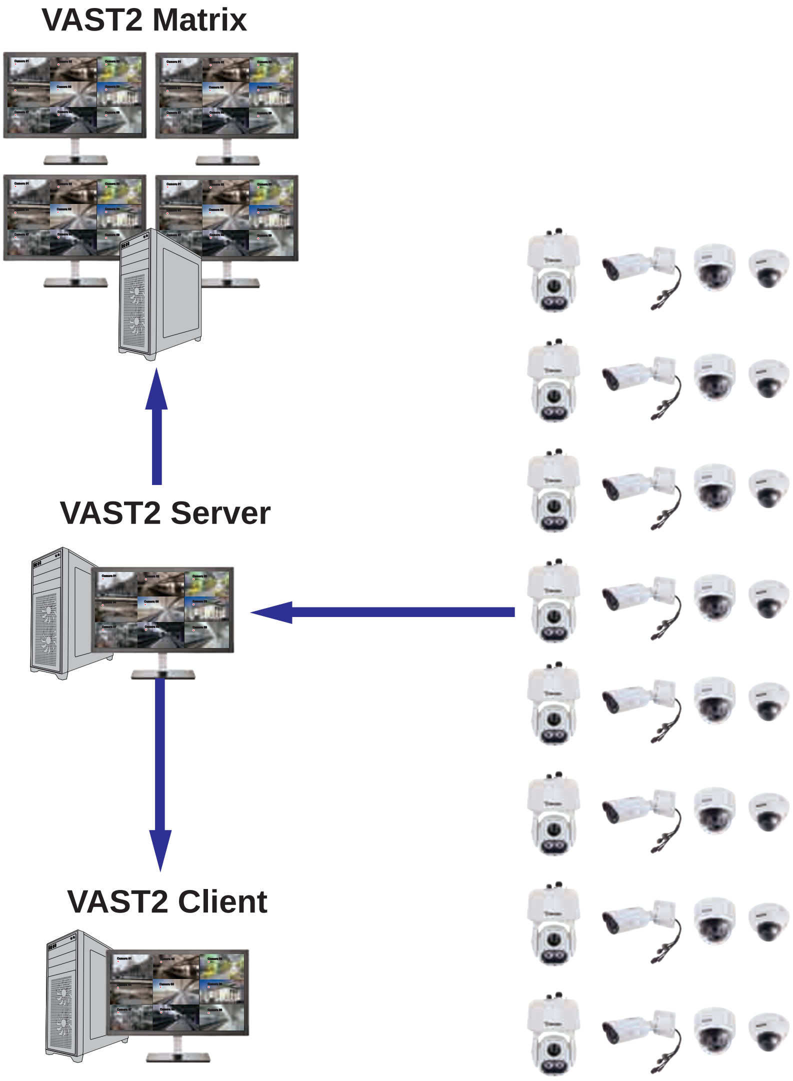
When the calibration is done, you can select different dewarp modes in VAST using the transition button on the upper right of the view cell.





Appendix C: 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.

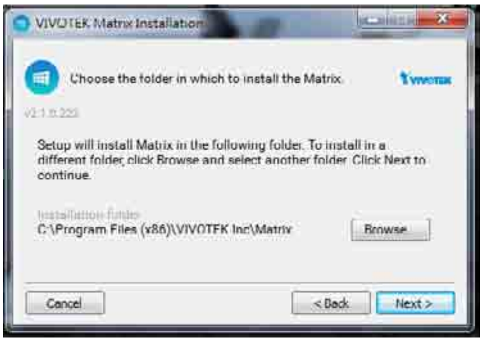


Prerequisites:

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:

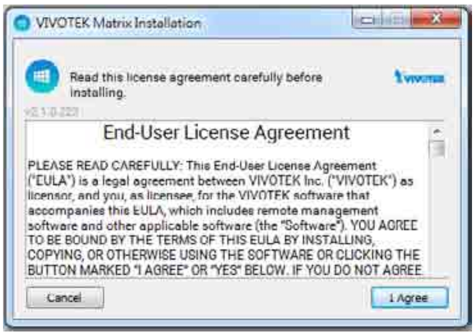
1. Install the Matrix client utility on a computer equipped with multiple monitors. Follow the onscreen instructions to install the utility.



Choose the folder in which to install the Matrix.

Setup will install Matrix in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

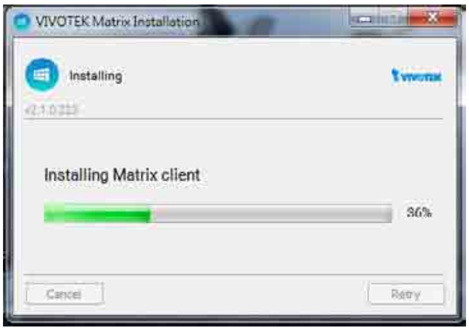
C:\Program Files (x86)\VIVOTEK Inc\Matrix



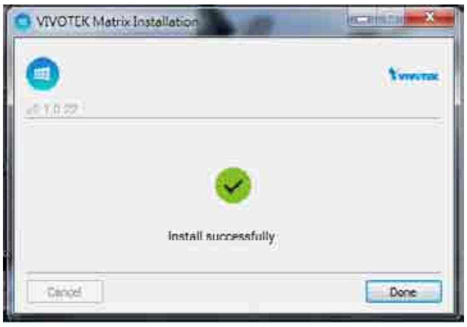
Read this license agreement carefully before installing.

End-User License Agreement

PLEASE READ CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between VIVOTEK Inc. ("VIVOTEK") as licensor, and you, as licensee, for the VIVOTEK software that accompanies this EULA, which includes remote management software and other applicable software (the "Software"). YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR OTHERWISE USING THE SOFTWARE OR CLICKING THE BUTTON MARKED "I AGREE" OR "YES" BELOW. IF YOU DO NOT AGREE

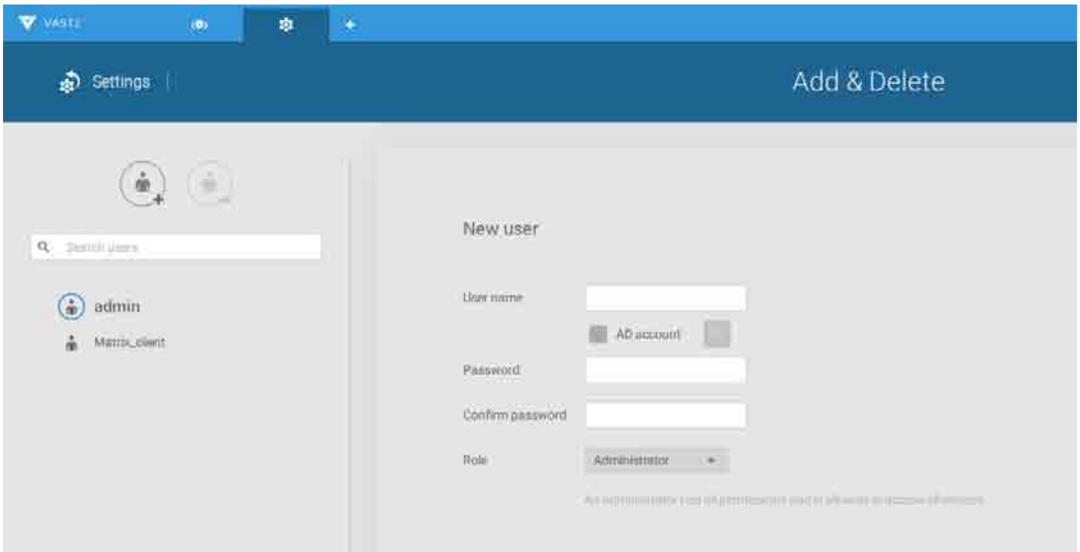


Installing Matrix client



Install successfully

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.



New user

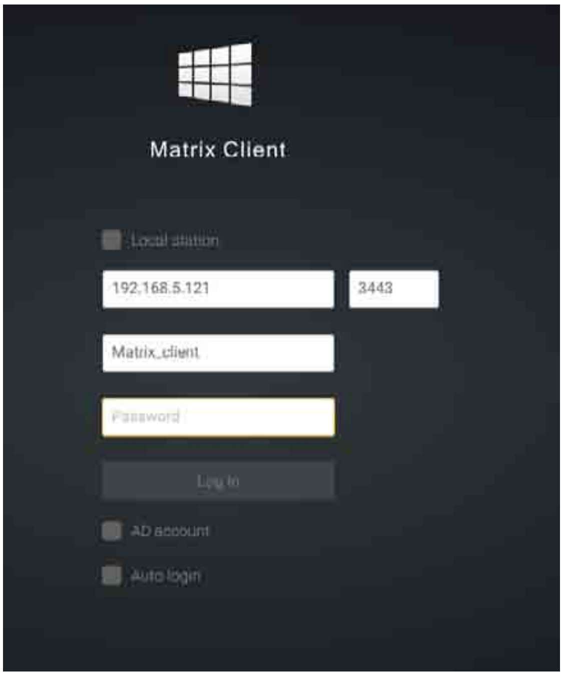
User name:

Password:

Confirm password:

Role: Administrator

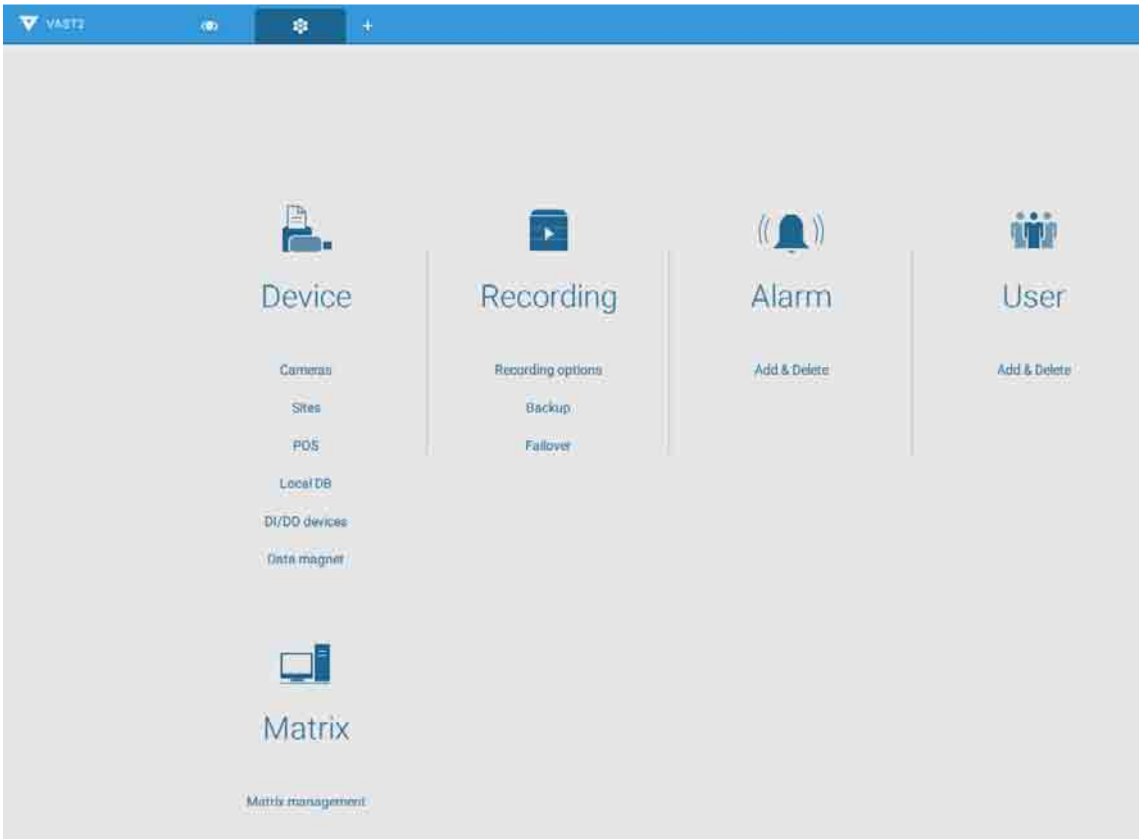
3. Open the Matrix utility, log in to the VAST server address, using the Matrix client account credentials.



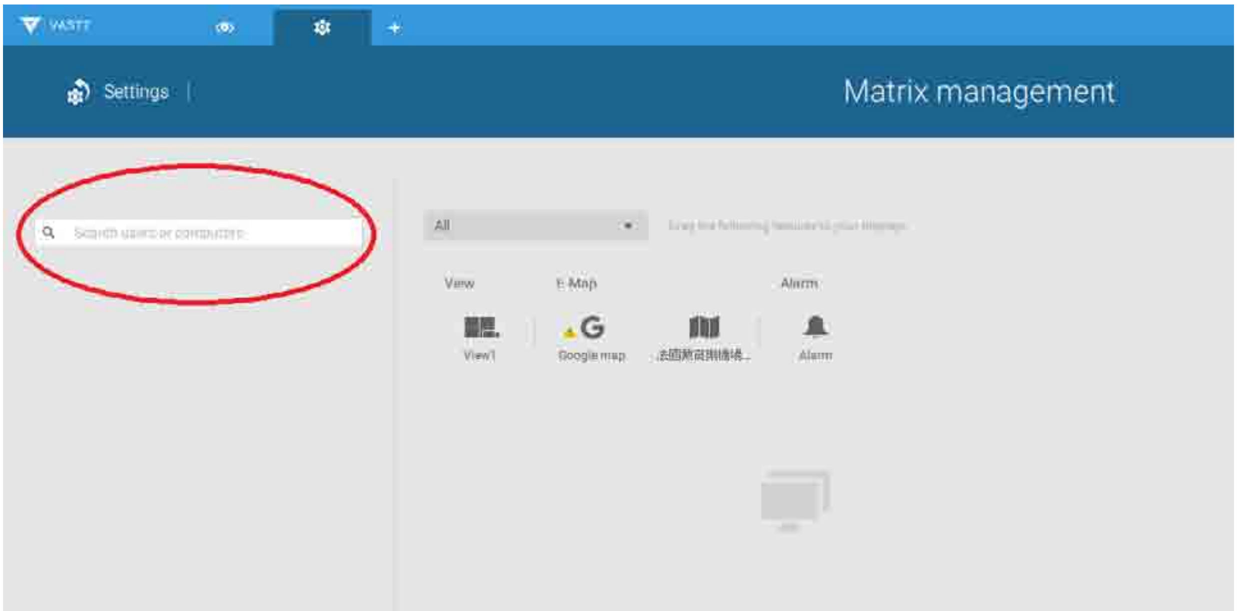
192.168.5.121 3443

Matrix_client

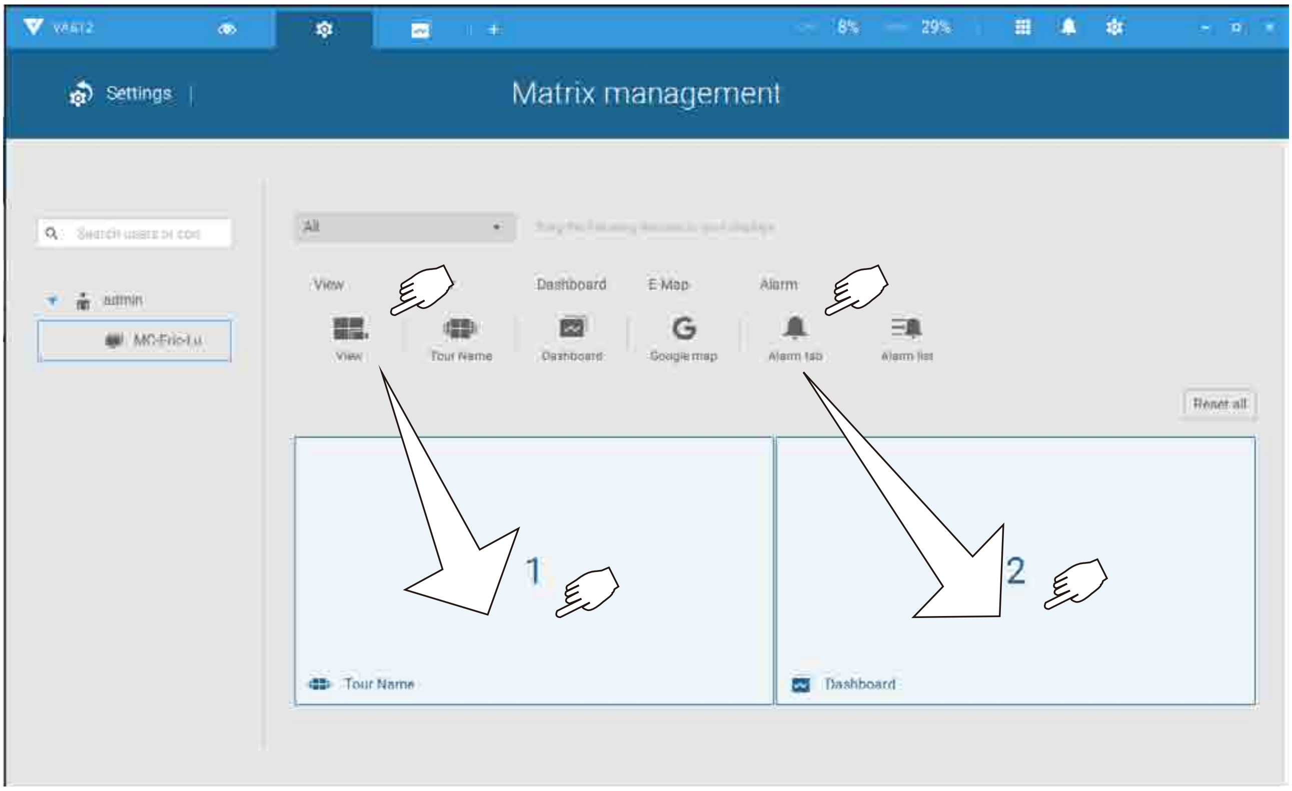
4. From the VAST server, open the Settings > Matrix Management window.



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).

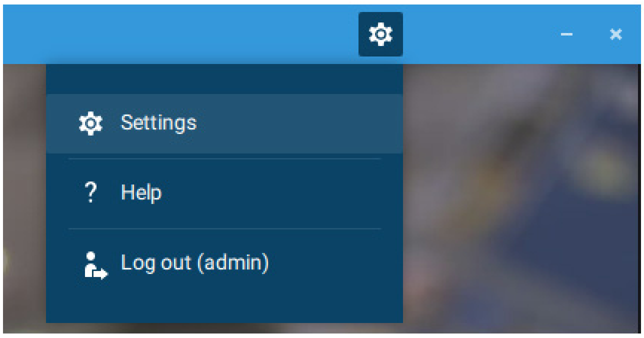

VAST
Settings
Matrix management
Search users or computers
All
Drag the following resources to your displays
View
E-Map
Alarm
View1
Google map
Alarm

6. Once the VAST server finds 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.

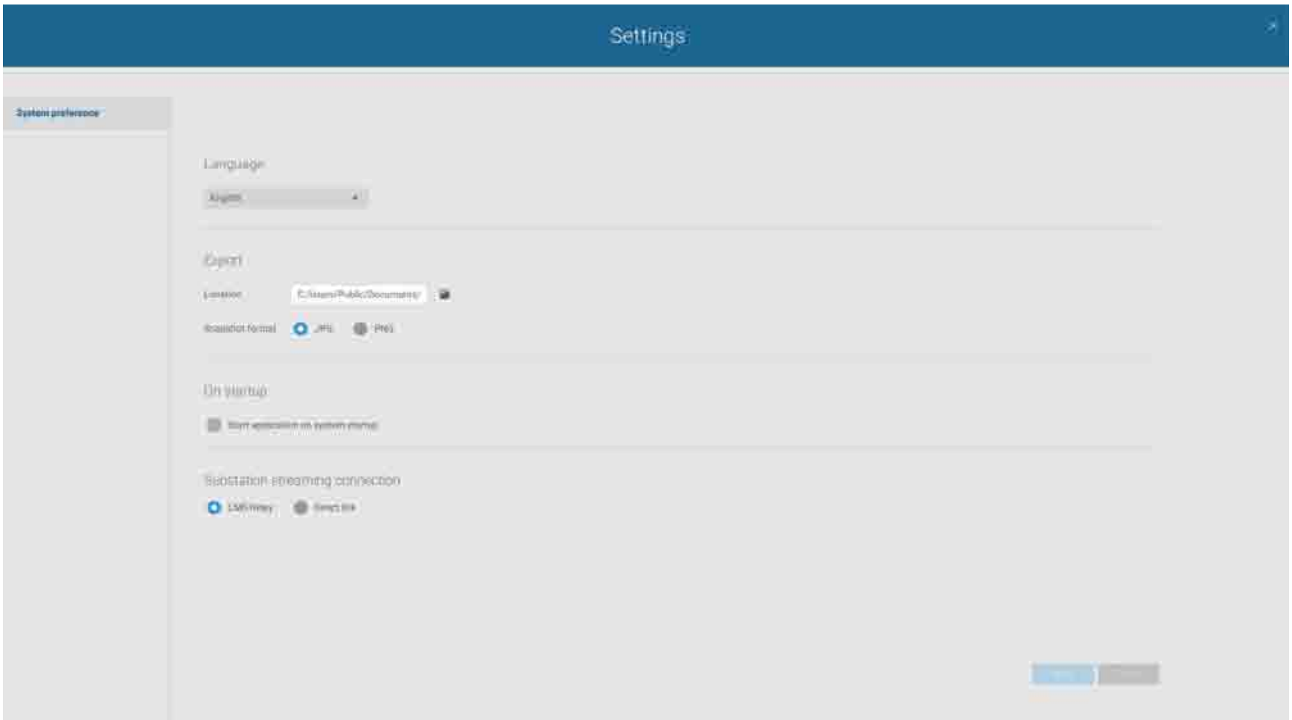


7. The views should immediately appear on the Matrix monitors.

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.



Settings

System preference

Language

English

Export

Location C:/Users/Public/Documents/

Snapshot format ◉ JPG ○ PNG

On startup

□ Start application on system startup

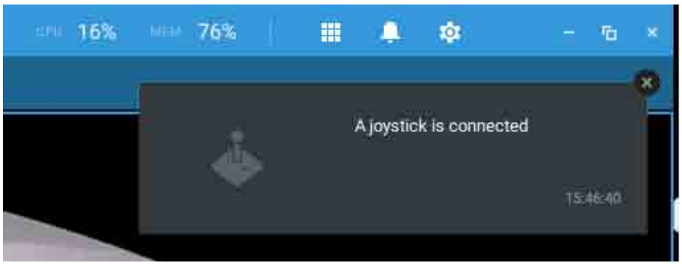
Substation streaming connection

◉ LMS relay ○ Direct link

Appendix D: Joystick Support

Configurable joystick buttons

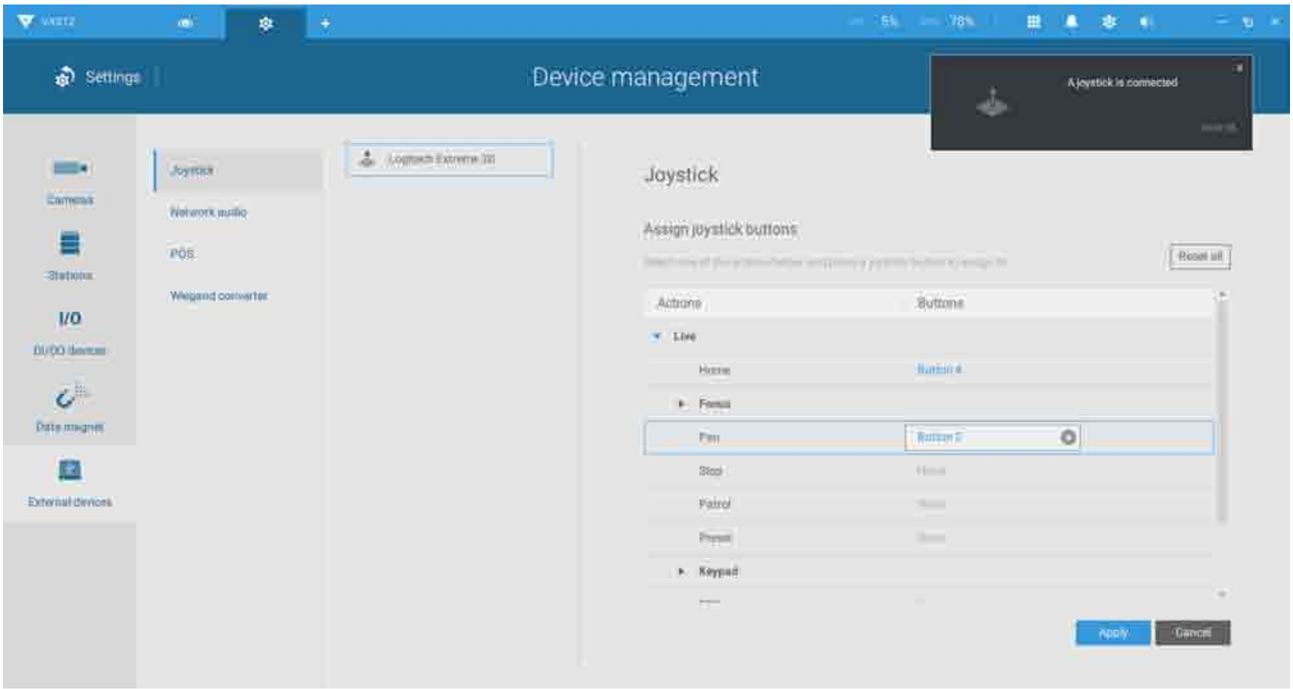
1. Connect the joystick's USB cable between the USB ports on the joystick and a VAST server/client.
2. Once connected, you should be prompted by a connection message.



A joystick is connected

15:46:40

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.



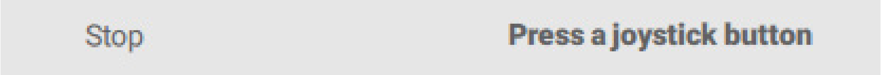
A joystick is connected

Joystick

Assign joystick buttons

Actions	Buttons
▼ Live	
Home	Button 4
▶ Focus	
Pan	Button 2
Stop	None
Patrol	None
Preset	None
▶ Keypad	

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

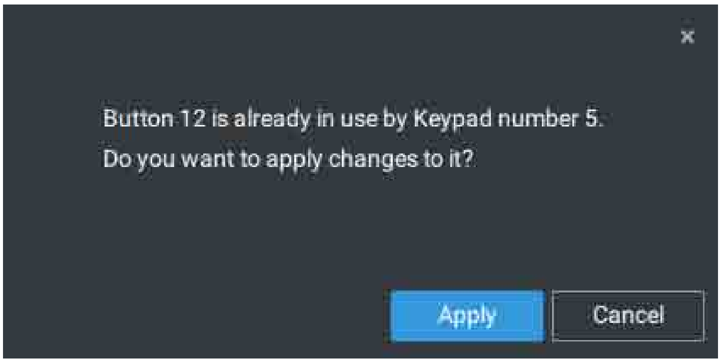


Stop

Press a joystick button

Press a preferred button on your joystick to complete the setting.

If a button conflict occurs, (another function has already been assigned to the same button), the below message will prompt. You can Cancel or click Apply to change the assignment.



Button 12 is already in use by Keypad number 5.
Do you want to apply changes to it?

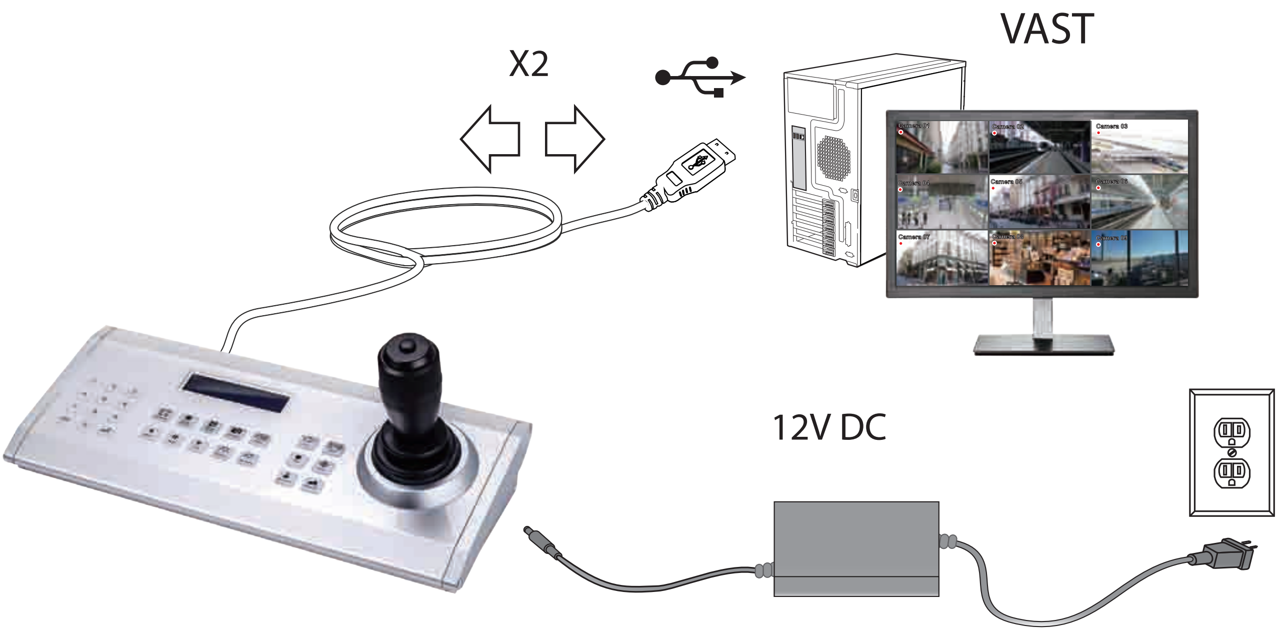
Repeat the above process and click the **Apply** button to preserve your settings.

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.

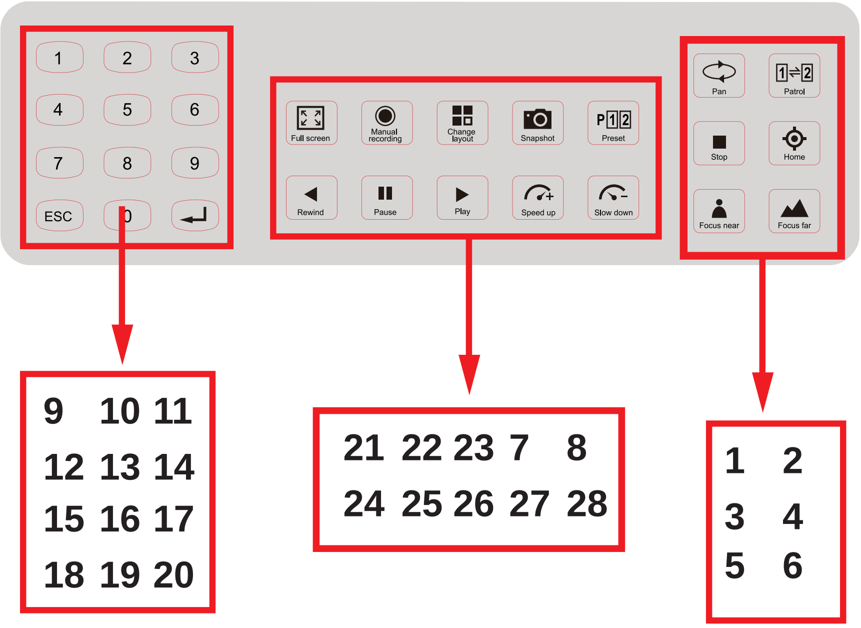


NOTE:

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

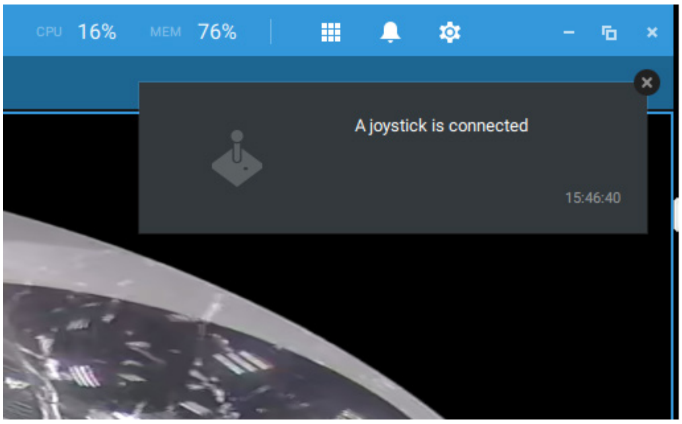
Below is the keypad numbering sequence:



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.



A joystick is connected

15:46:40

The following controls are available:

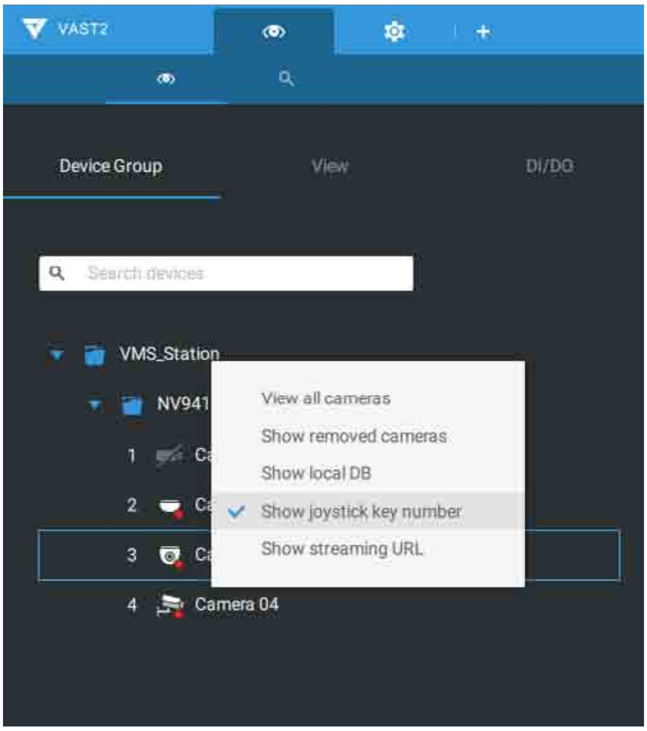
* PTZ control – Basic PTZ control: Direction, Home, Zoom in/out, and Focus near/far.

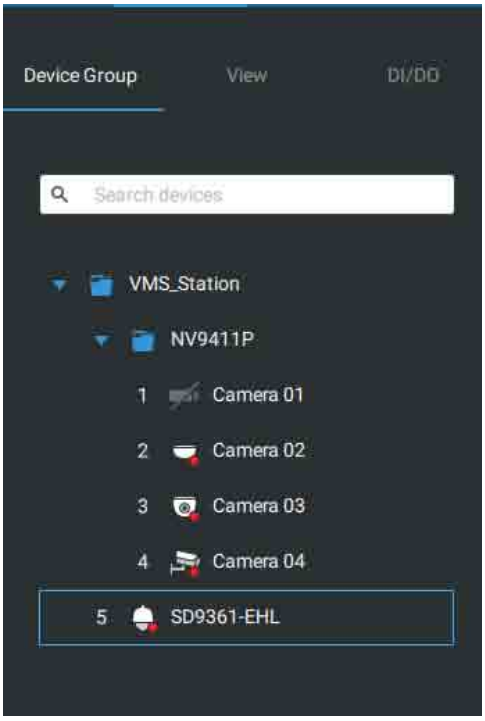
* Playback control – Play, Pause, Stop, Rewind, Speed up and Slow down.

* 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.

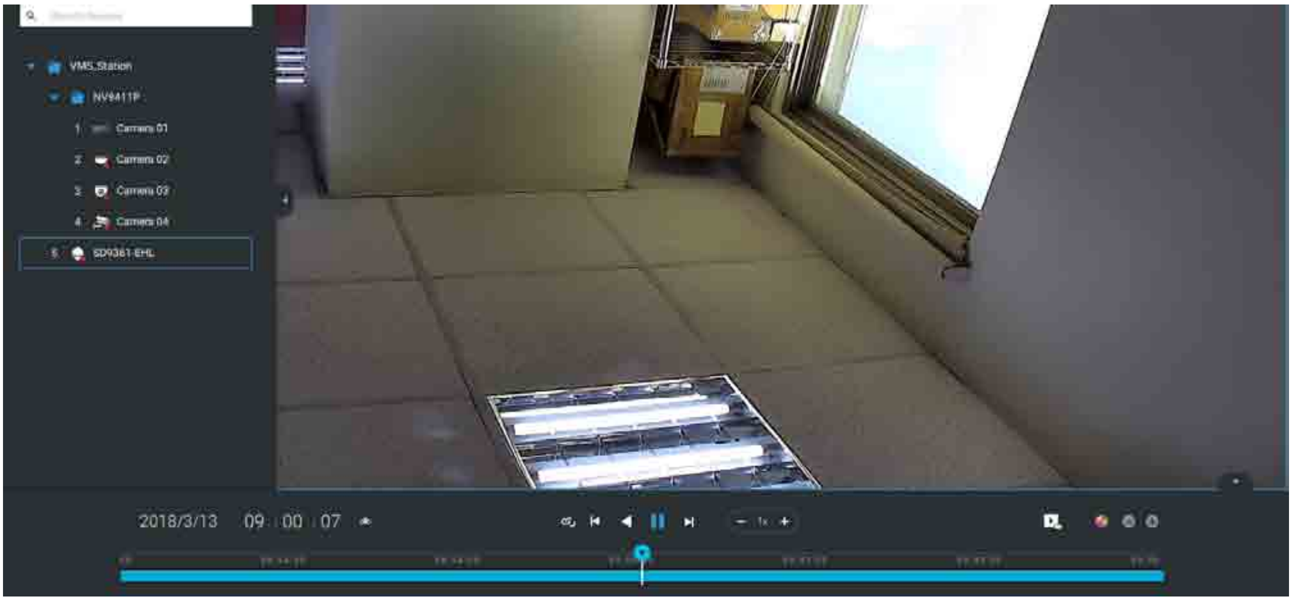
To move to a preset position, press the number key + Preset, and the Enter key ↵. The number key corresponds to the sequence number for the preset position regardless of the name of the preset.

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).

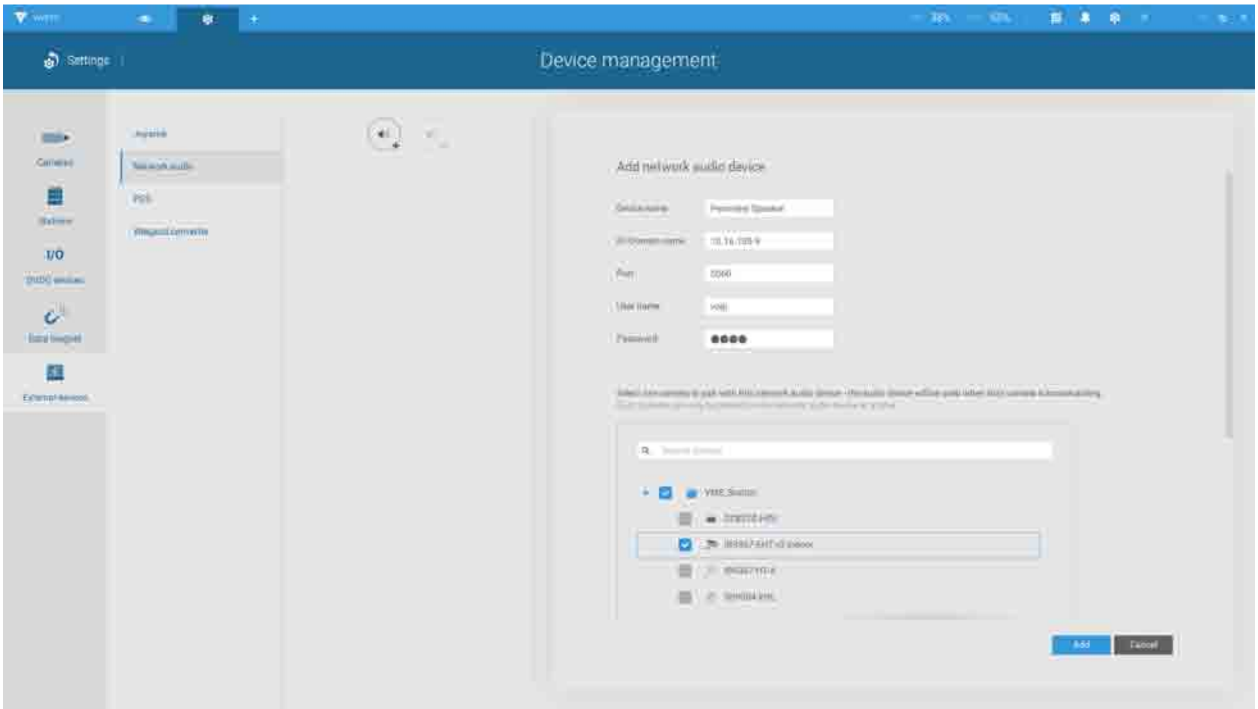
The Play button toggles the playback window. From here you can trace back the past recordings. You can use speed up, slow down, and rewind buttons here. Once the Playback mode is toggled, the point-in-time defaults to the start of the current hour.



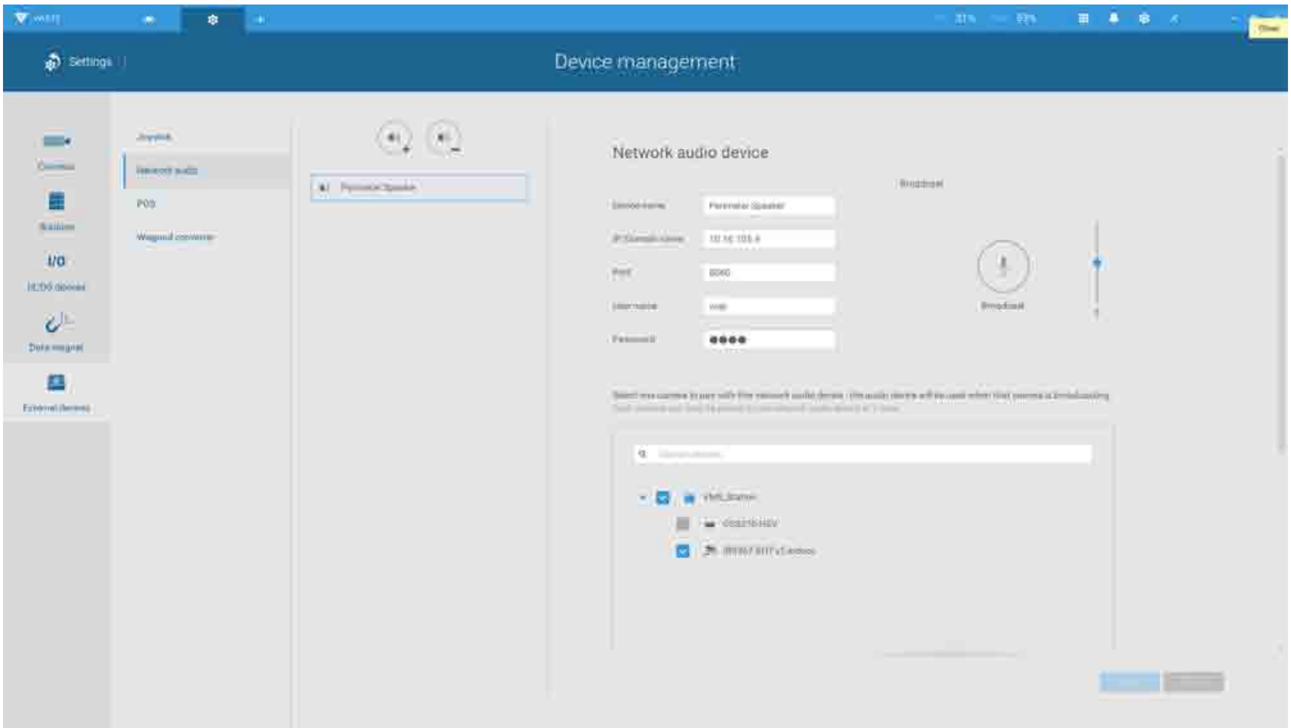
Appendix E: Network Audio Solution

You can add network speakers to your workstation in Settings > External Devices > Network Audio.

1. Connect the network speaker to a local network.
2. Once connected, enter its IP address, User Name, Password, Port number (default is 5060).
3. You can associate one network camera with the speaker.

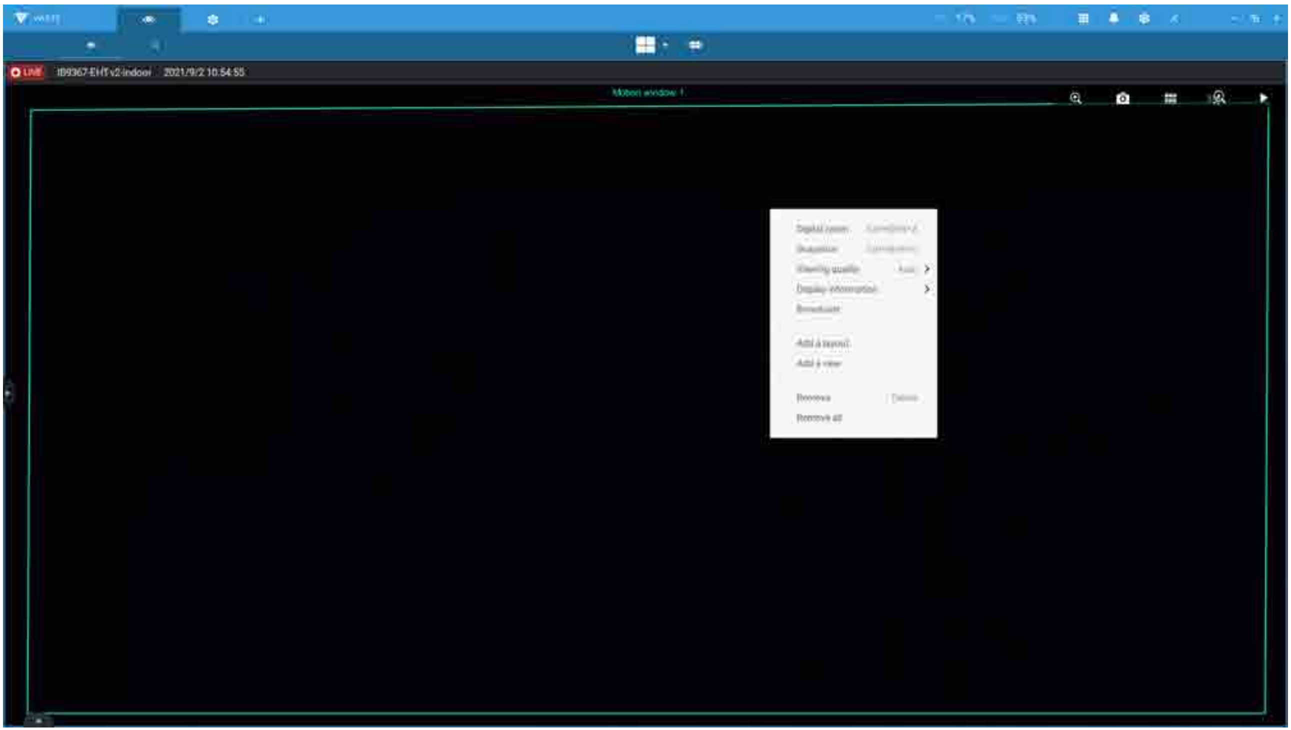


4. You can use the Broadcast function on the right of the screen to test the connectivity.
5. You can right-click on the live view to find the Broadcast function to speak or broadcast a audio clip.

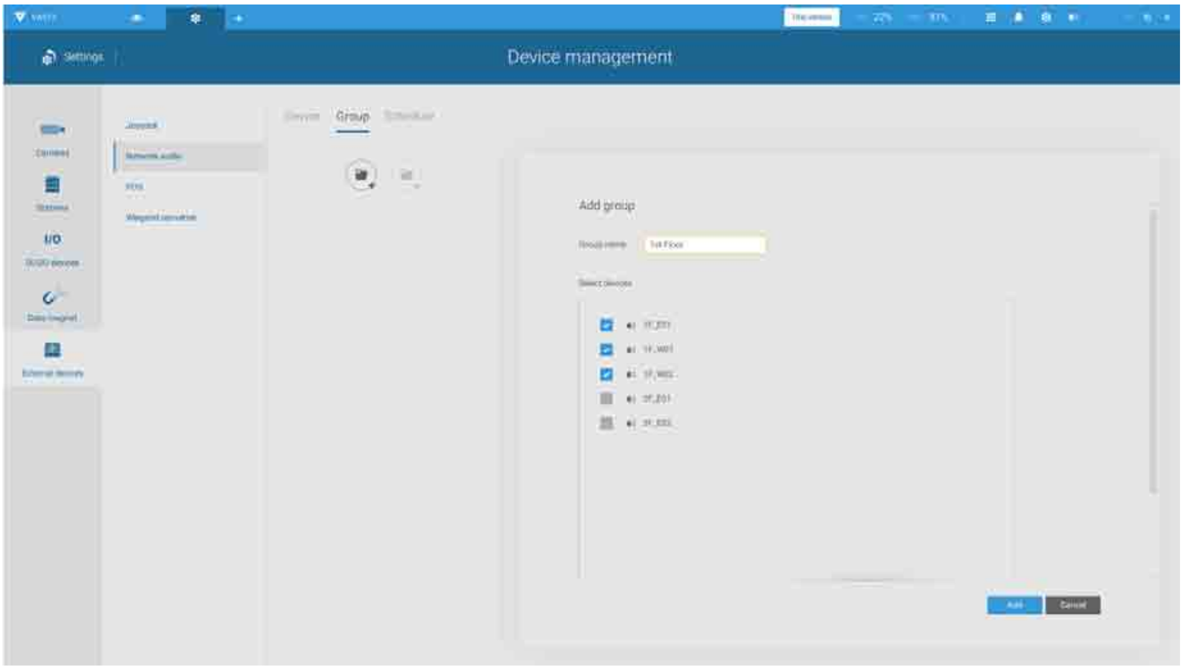


6. On the occurrence of a triggered alarm (Motion or VCA event), you can configure the alarm settings so that system can broadcast an audio clip. Configure audio clip settings in System > Media, and select "Play audio file with network audio device" in the Alarm action page.

Note that the pre-recorded audio clip should be uploaded from System > Media. The supported audio file is WAV: 8Khz, Mono, 16-bit, PCM.



You can create groups for different audio devices. Use the Group tab to create audio groups. Select devices for the group.



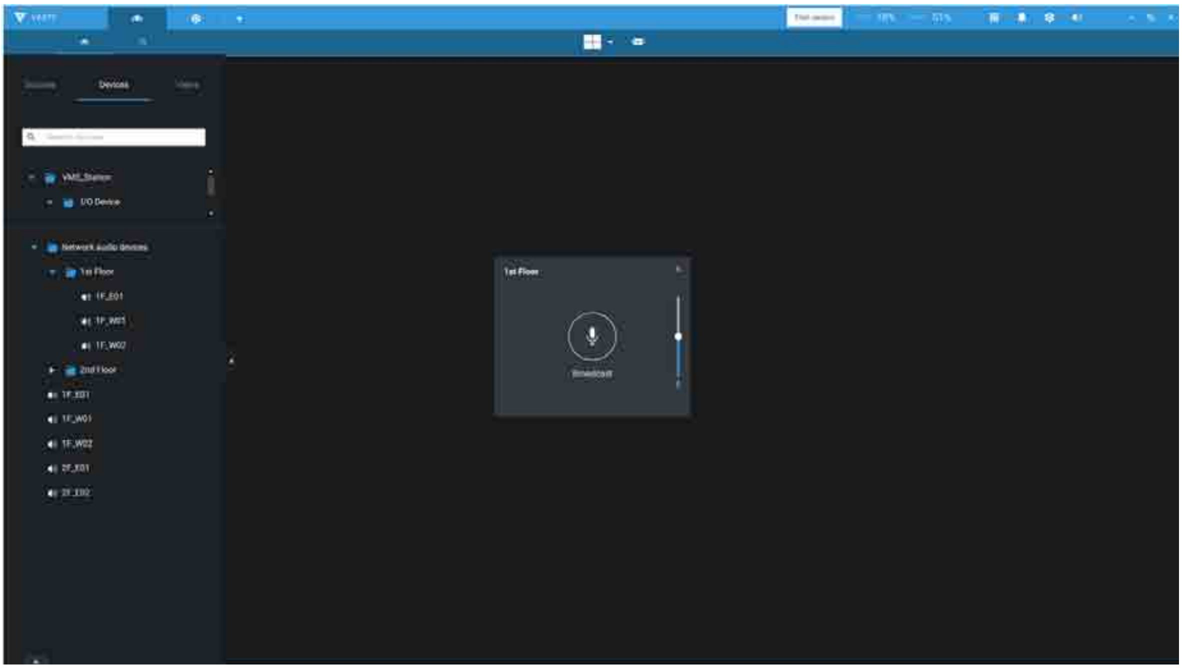
Add group

Group name: 1st Floor

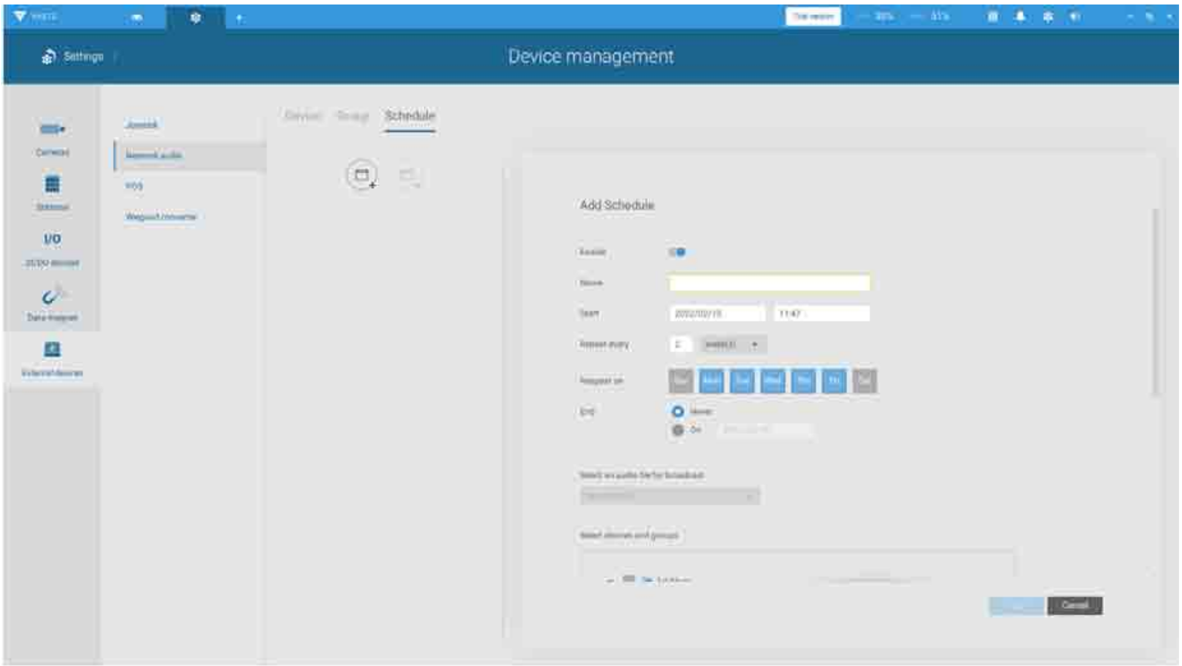
Select devices

☑ 1F_E01
☑ 1F_W01
☑ 1F_W02
□ 2F_E01
□ 2F_E02

With audio groups, you can select audio devices from the Devices tab on a live view so that you can broadcast audios to a group of devices.



You can create a schedule to play a pre-selected audio file. In Network aduio > schedule, create a schedule. Select a start time. Select an audio file for broadcast. Select a repeating pattern by hour, by day, or by the week days. You can also specify an audio group to play by the schedule.



Add Schedule

Enable ●

Name

Start 2022/02/15 11:47

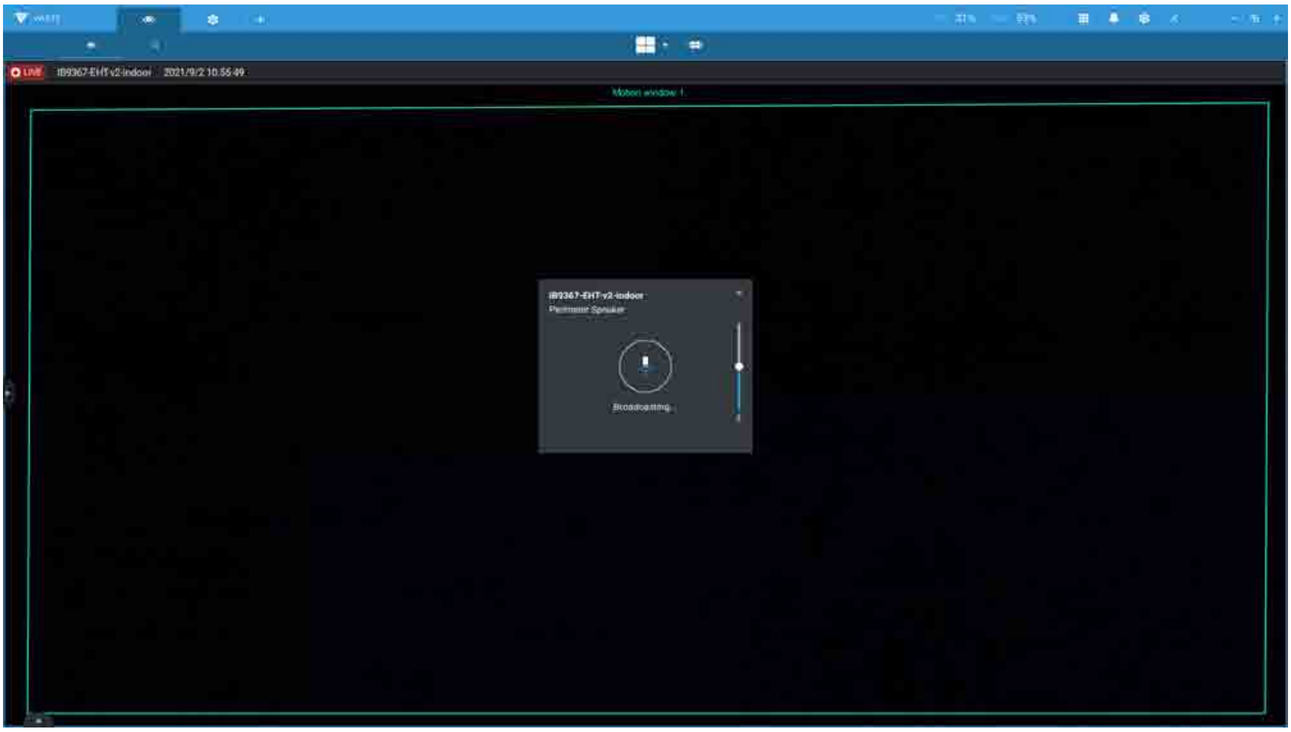
Repeat every 1 week(s)

Repeat on Sun Mon Tue Wed Thu Fri Sat

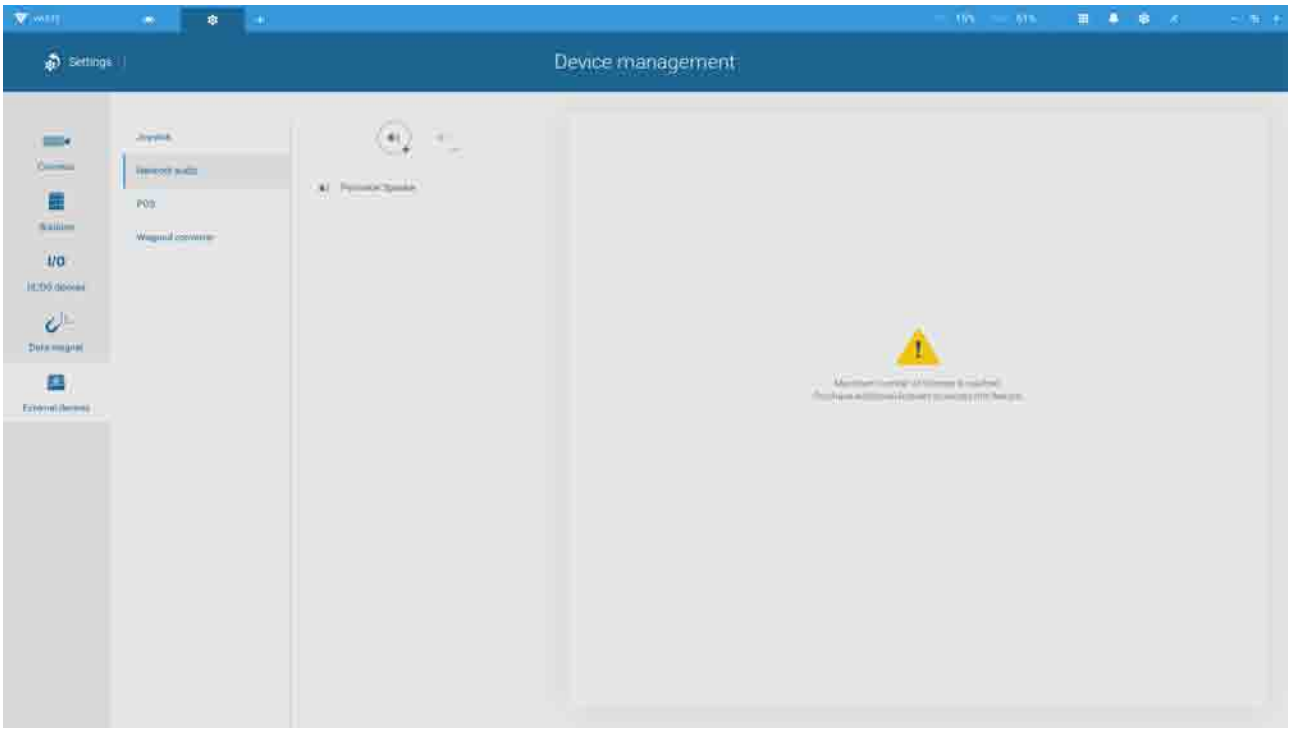
End ● Never ○ On

Select an audio file for broadcast

Select devices and groups



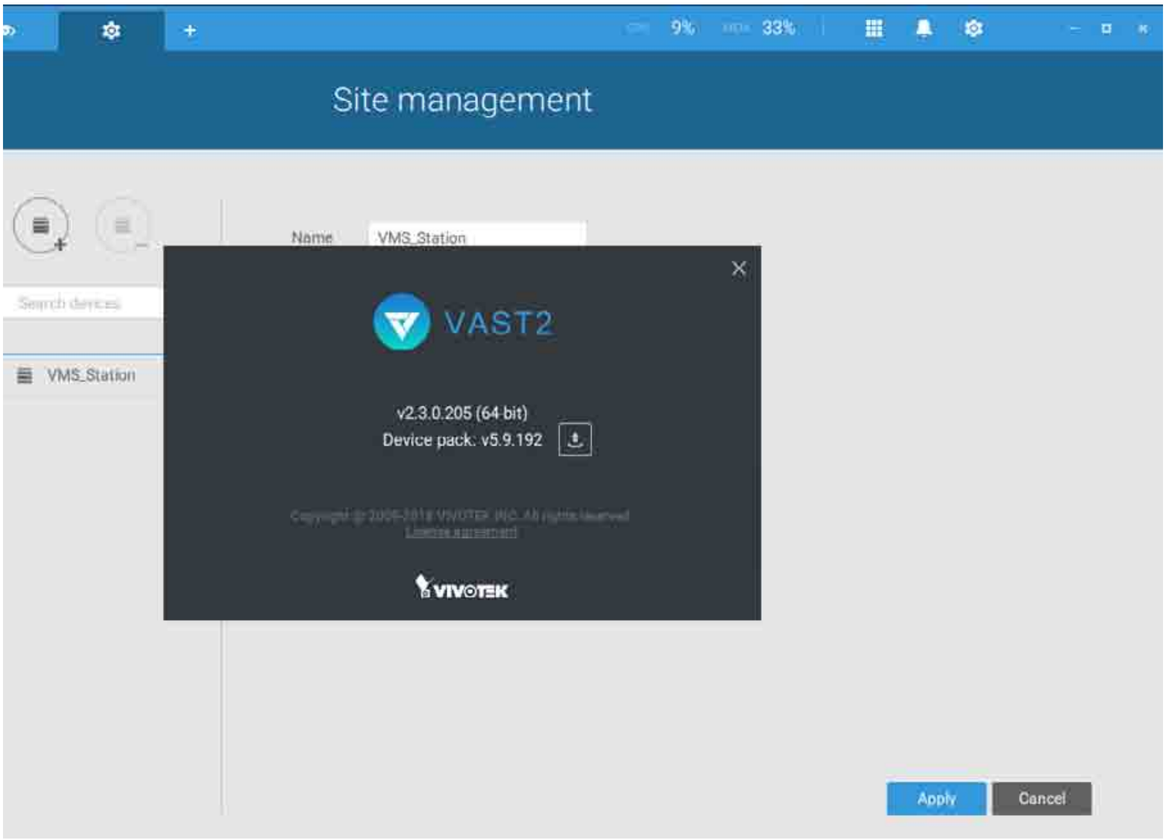
7. Note that network audio is a purchased feature. Please contact VIVOTEKs sales representatives for the extension licenses.



Appendix F: 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.

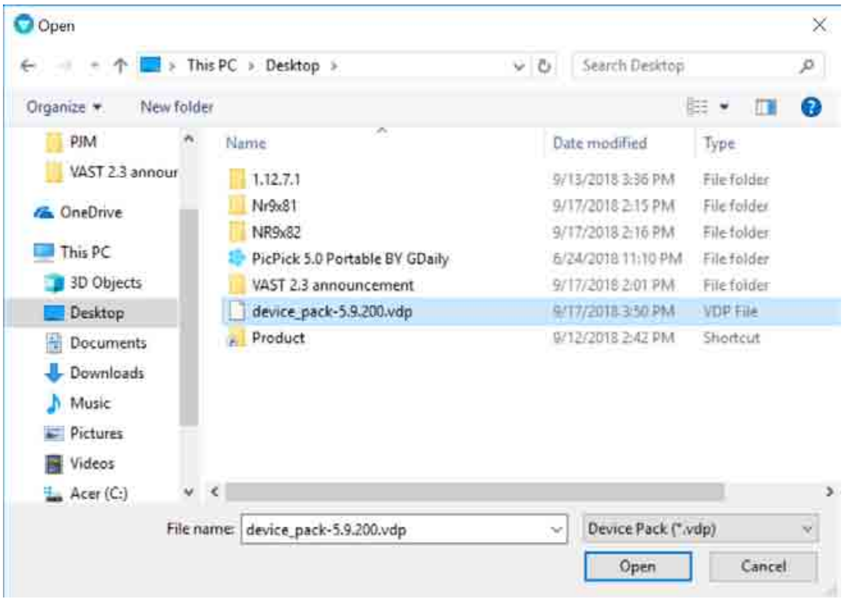


Name VMS_Station

v2.3.0.205 (64-bit)
Device pack: v5.9.192

Copyright © 2005-2018 VIVOTEK INC. All rights reserved
License agreement

A device pack file looks like the following.



Name	Date modified	Type
1.12.7.1	9/13/2018 3:36 PM	File folder
Nr9x81	9/17/2018 2:15 PM	File folder
NR9x82	9/17/2018 2:16 PM	File folder
PicPick 5.0 Portable BY GDaily	6/24/2018 11:10 PM	File folder
VAST 2.3 announcement	9/17/2018 2:01 PM	File folder
device_pack-5.9.200.vdp	9/17/2018 3:50 PM	VDP File
Product	9/12/2018 2:42 PM	Shortcut

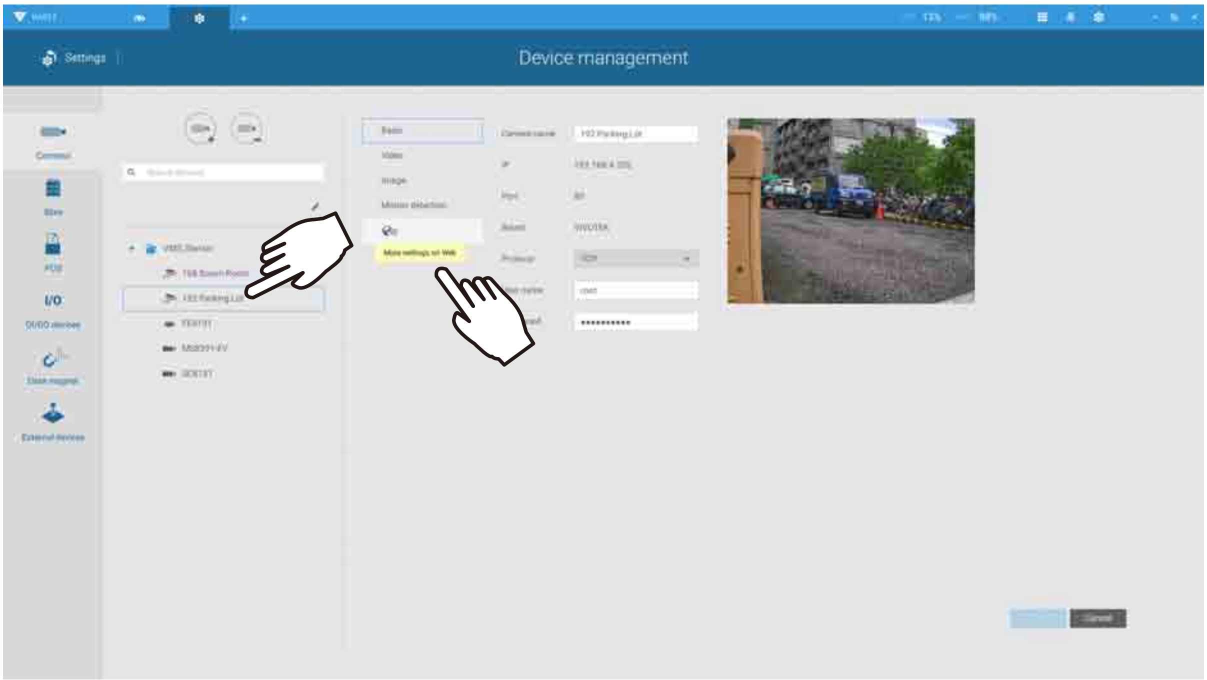
File name: device_pack-5.9.200.vdp

Device Pack (*.vdp)

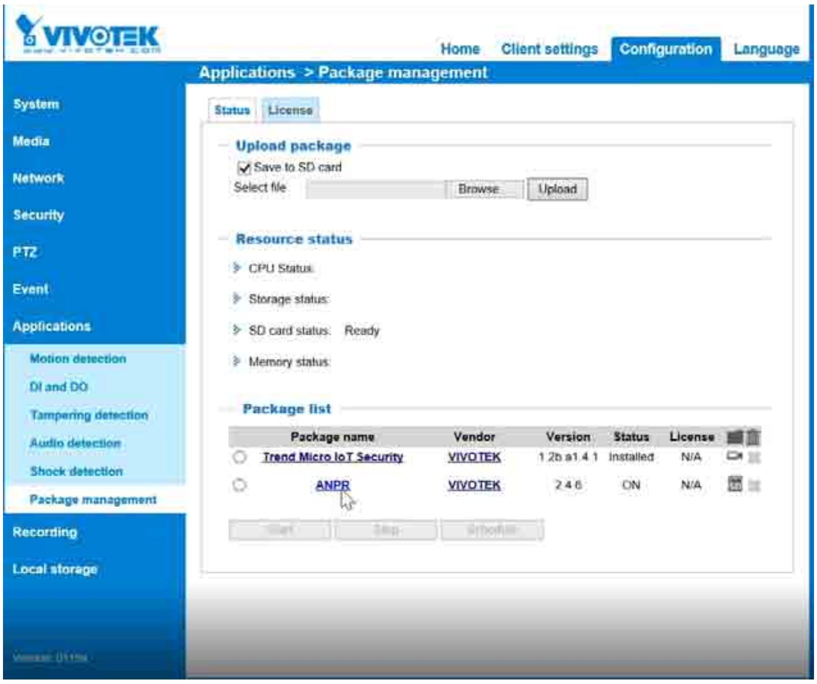
Appendix G: Using LPR Related Functions w/ Data Magnet

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.



Upload package

☑ Save to SD card

Select file

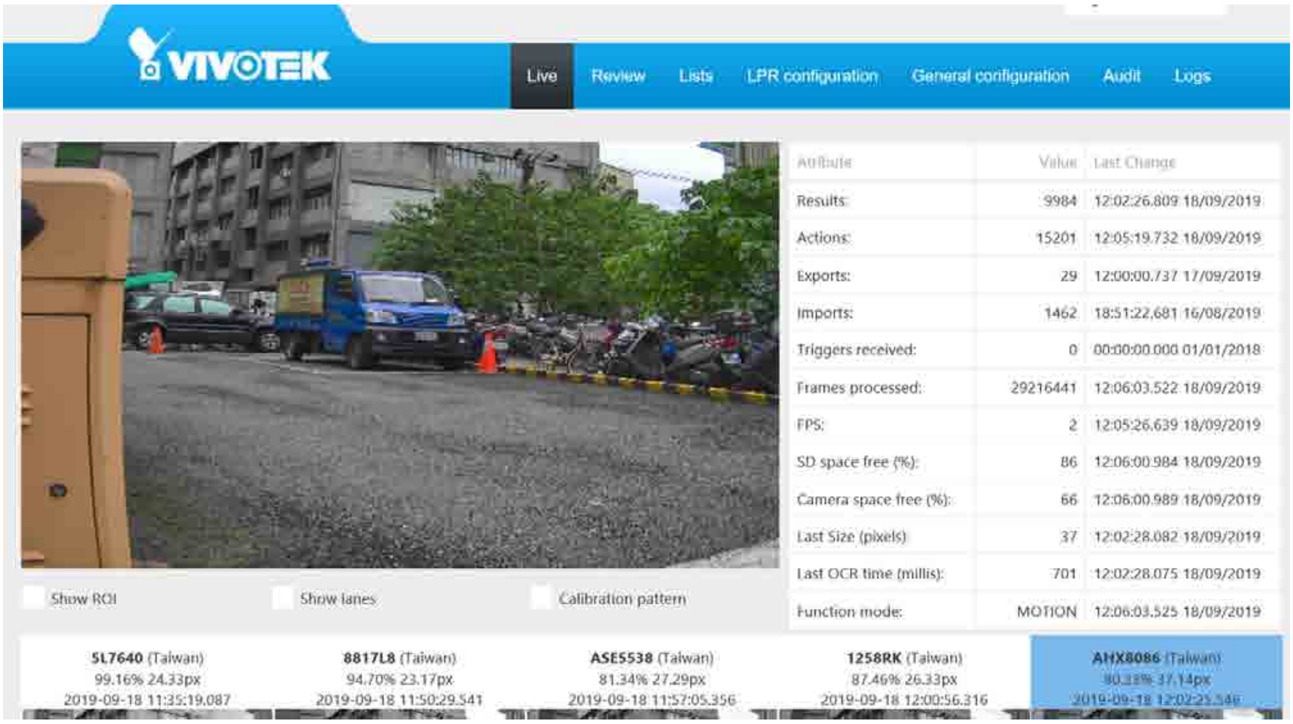
Resource status

- CPU Status:
- Storage status:
- SD card status: Ready
- Memory status:

Package list

	Package name	Vendor	Version	Status	License
○	Trend Micro IoT Security	VIVOTEK	1.2b.a1.4.1	Installed	N/A
○	ANPR	VIVOTEK	2.4.6	ON	N/A

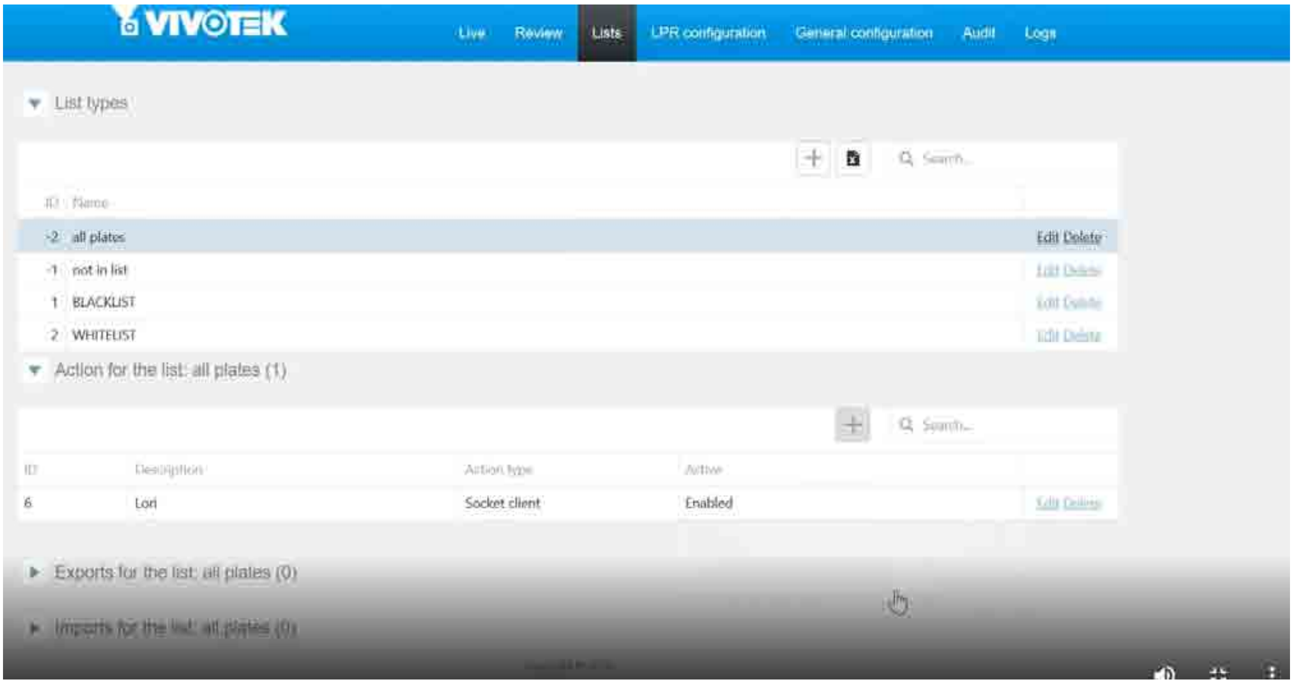
3. Click on the **Lists** tab.



Attribute	Value	Last Change
Results:	9984	12:02:26.809 18/09/2019
Actions:	15201	12:05:19.732 18/09/2019
Exports:	29	12:00:00.737 17/09/2019
Imports:	1462	18:51:22,681 16/08/2019
Triggers received:	0	00:00:00.000 01/01/2018
Frames processed:	29216441	12:06:03.522 18/09/2019
FPS:	2	12:05:26.639 18/09/2019
SD space free (%):	86	12:06:00.984 18/09/2019
Camera space free (%):	66	12:06:00.989 18/09/2019
Last Size (pixels)	37	12:02:28.082 18/09/2019
Last OCR time (millis):	701	12:02:28.075 18/09/2019
Function mode:	MOTION	12:06:03.525 18/09/2019

5L7640 (Taiwan) 99.16% 24.33px 2019-09-18 11:35:19.087	**8817L8** (Taiwan) 94.70% 23.17px 2019-09-18 11:50:29.541	**ASE5538** (Taiwan) 81.34% 27.29px 2019-09-18 11:57:05.356	**1258RK** (Taiwan) 87.46% 26.33px 2019-09-18 12:00:56.316	**AHX8086** (Taiwan) 90.33% 37.14px 2019-09-18 12:02:25.546

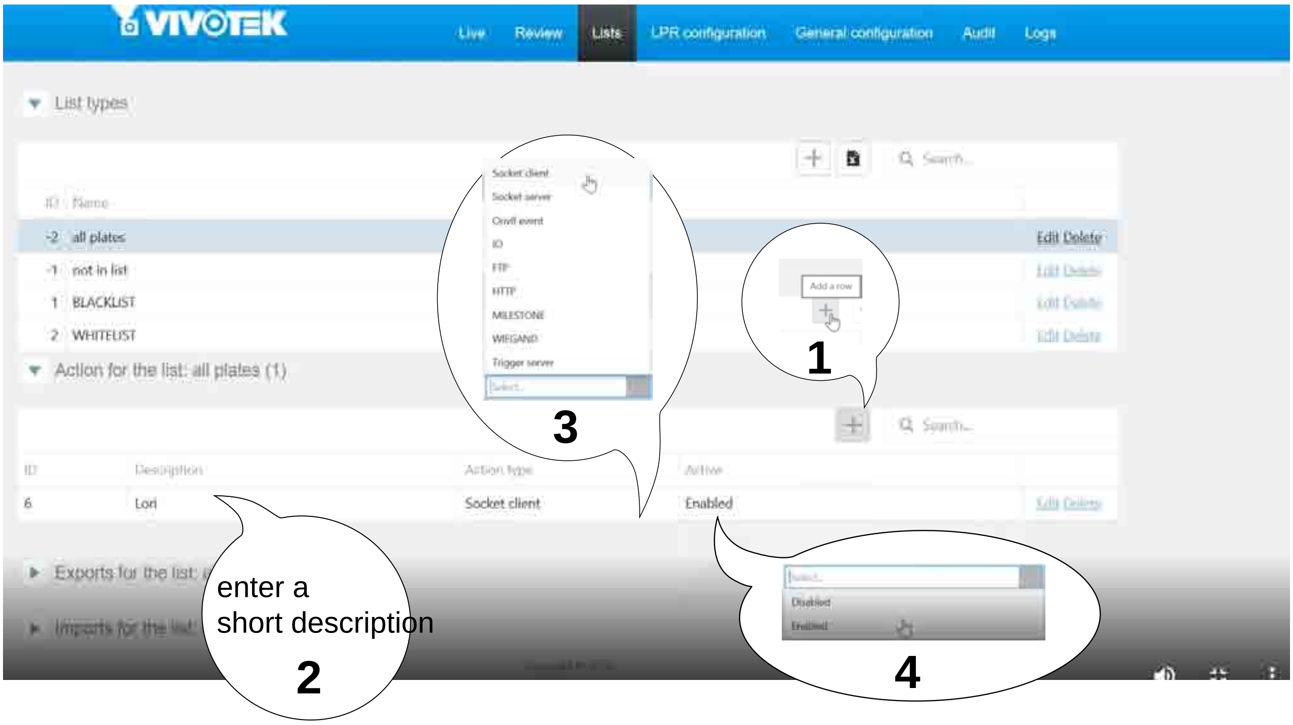
4. Select a list whose data will be transmitted to the VAST server.


VIVOTEK
Live
Review
Lists
LPR configuration
General configuration
Audit
Logs
List types
Search...
Action for the list: all plates (1)
Search...
Exports for the list: all plates (0)
Imports for the list: all plates (0)

ID	Name	
-2	all plates	Edit Delete
-1	not in list	Edit Delete
1	BLACKLIST	Edit Delete
2	WHITELIST	Edit Delete

ID	Description	Action type	Active	
6	Lori	Socket client	Enabled	Edit Delete

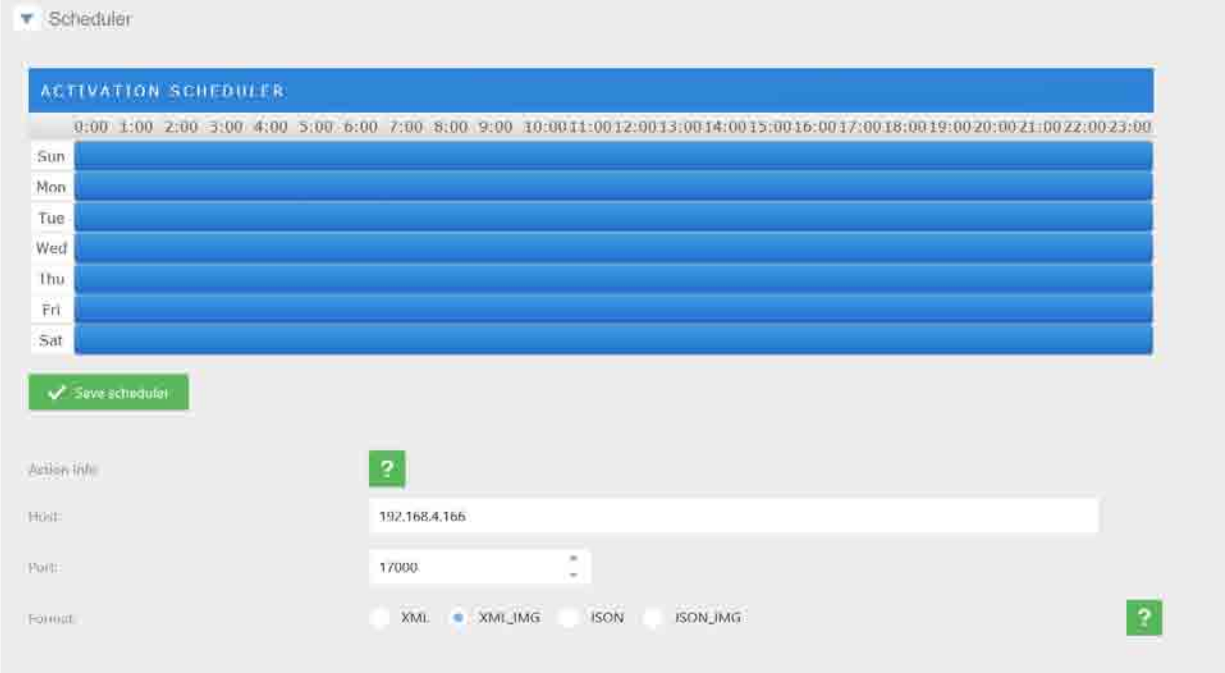
5. 5-1. Find the "Action for the list" pane. Click the "**+**" **Add a row** button.
   5-2. Enter a short description for the row.
   5-3. Select "**Socket client**" as the action type.
   5-4. Click to select **Enabled**.
   5-5. Click the **Save** button.



ID	Name	
-2	all plates	Edit Delete
-1	not in list	Edit Delete
1	BLACKLIST	Edit Delete
2	WHITELIST	Edit Delete

ID	Description	Action type	Active	
6	Lori	Socket client	Enabled	Edit Delete

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.



Action info:

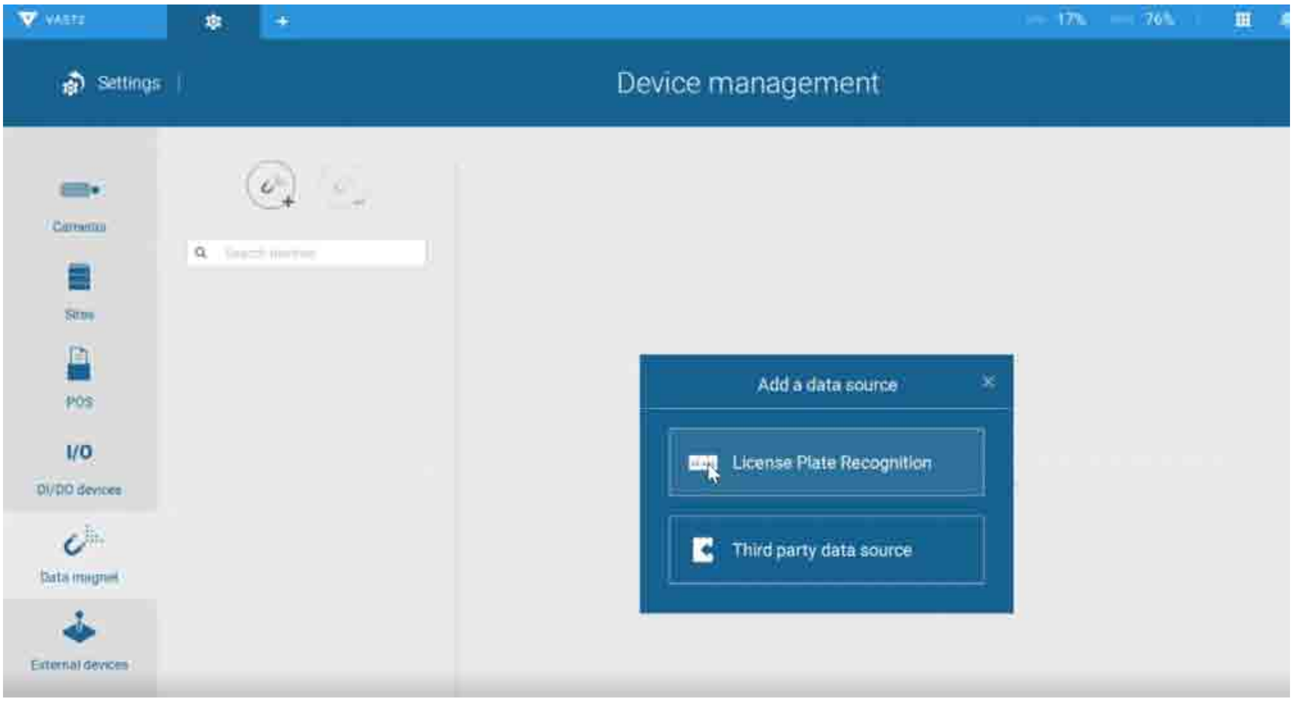
Host: 192.168.4.166

Port: 17000

Format: ○ XML ● XML_IMG ○ JSON ○ JSON_IMG

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.

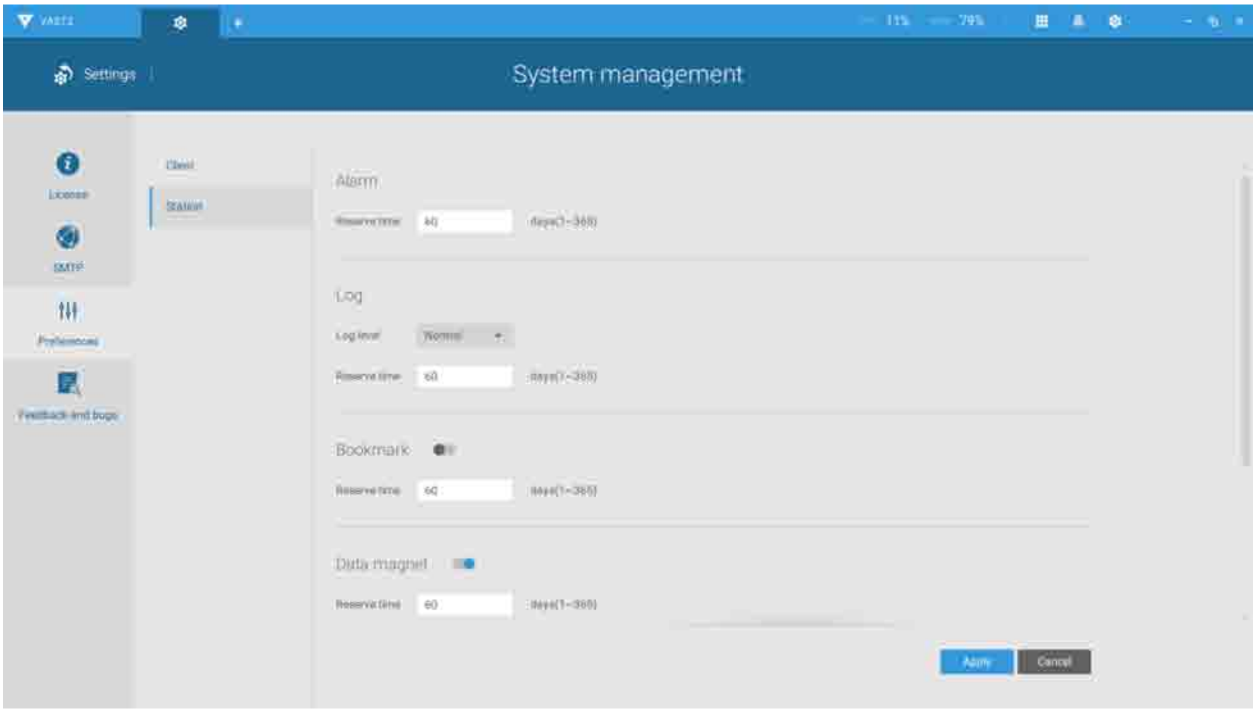


NOTE:

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**.



Alarm
Reserve time 60 days(1~365)

Log
Log level Normal
Reserve time 60 days(1~365)

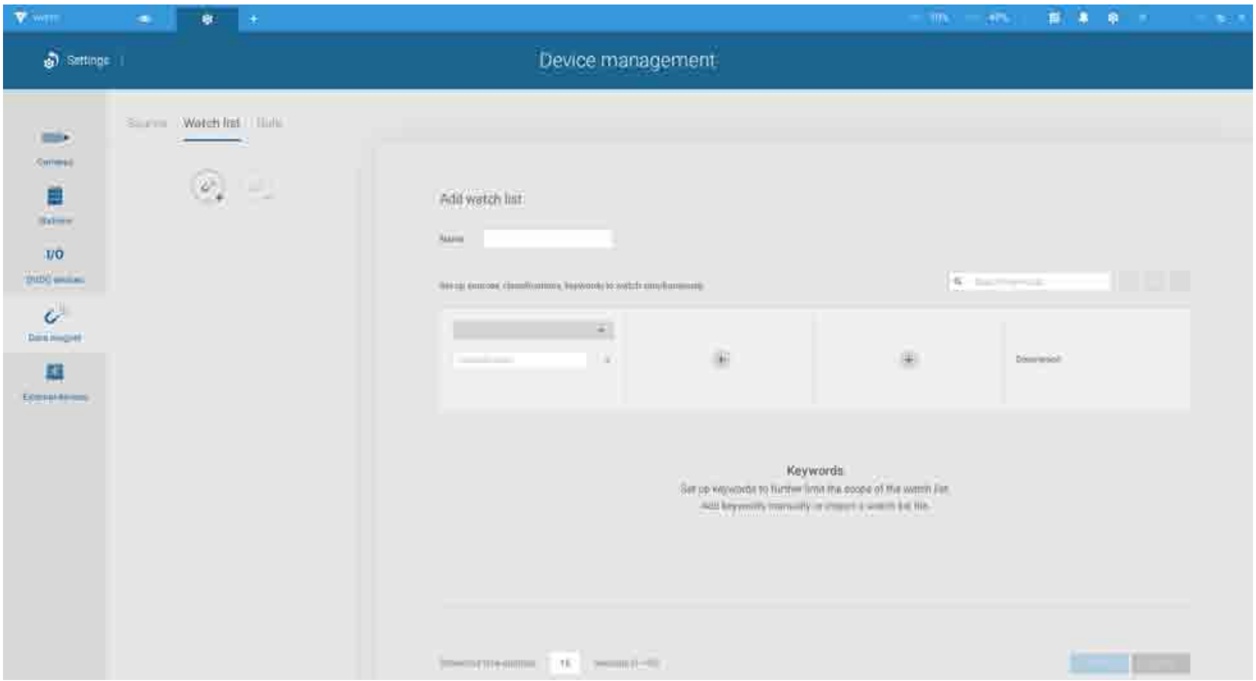
Bookmark
Reserve time 60 days(1~365)

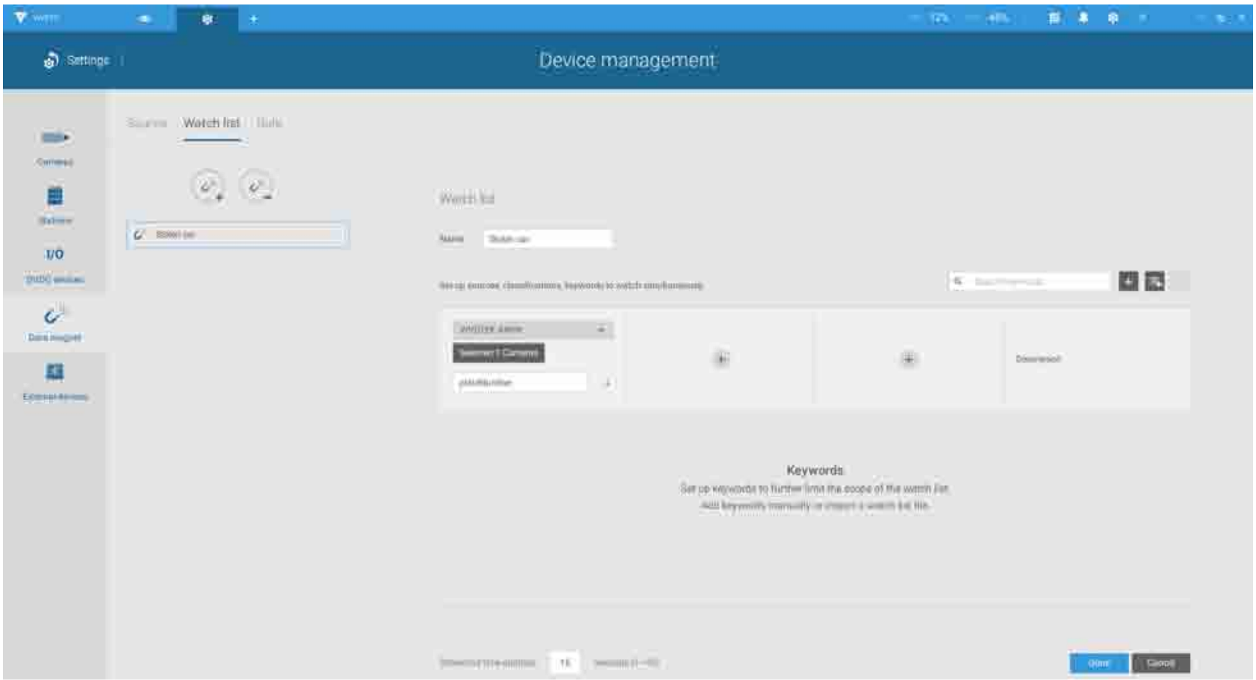
Data magnet
Reserve time 60 days(1~365)

Configuring a Black or White list:

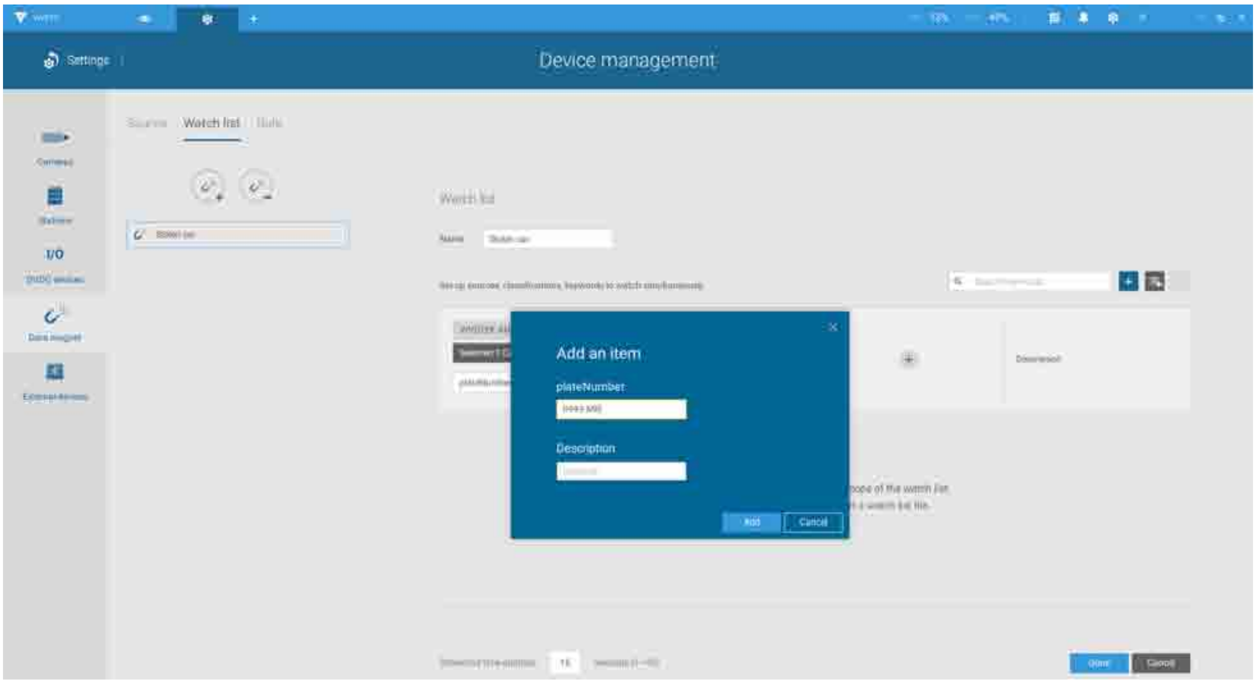
With a license plate application, you can configure either a Black list for suspicious plate numers, such as those for unwelcome or stolen cars, or a White list for VIP customers or the employees of your facility.

1. Click and select Watch list in the Data Magnet window. Click the Add button, and enter a name, e.g., Stolen car. Select "VIVOTEK ANPR" and camera as a data source, and enter a classification for the referential parameter in your Data Magnet json, e.g., PlateNumber.

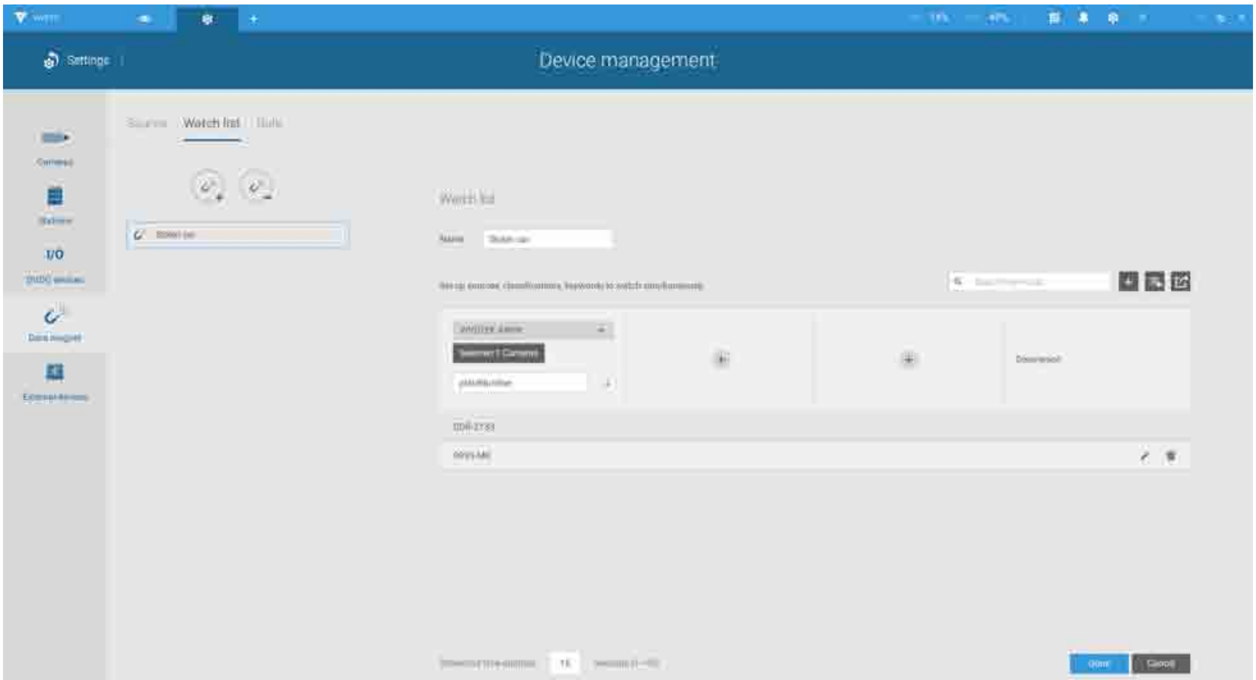




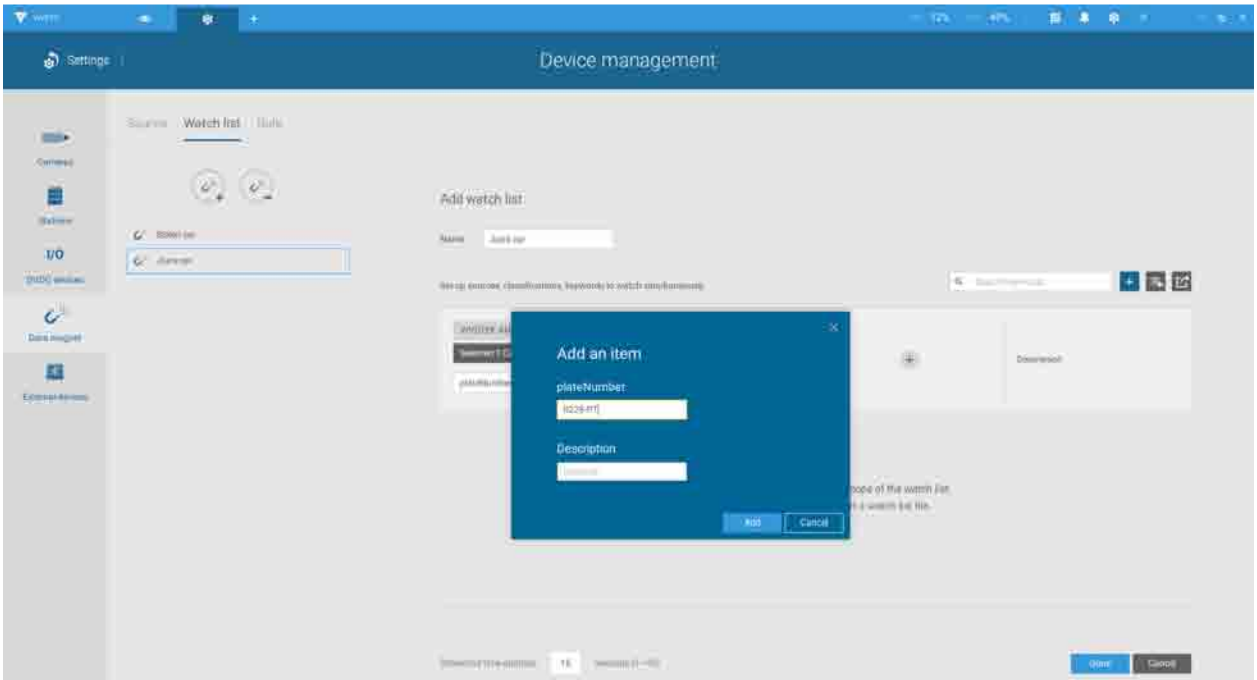
2. Click the Add + button and enter a plate number such as one for a stolen car. Click Add to finish, and repeat the process for more items.



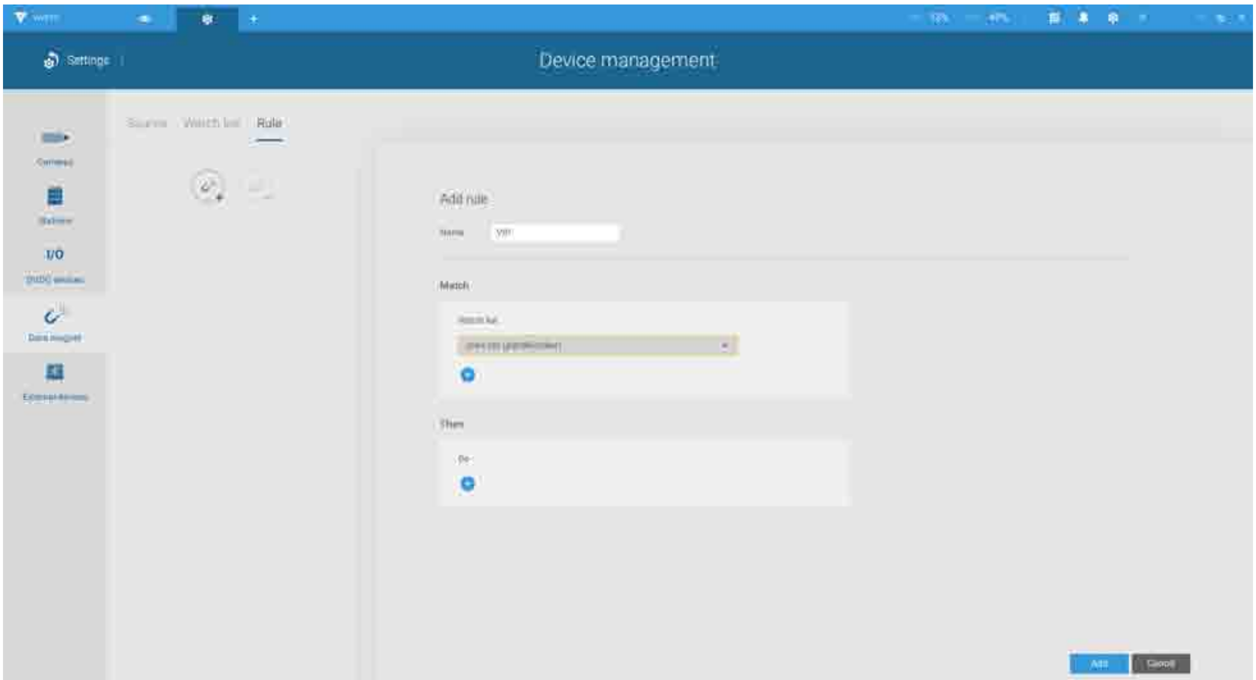
3. The added items will be listed. When done, click the Done button below.



4. Using the same method, you can create a White list for some plate numbers to gain access, such as VIP customers.



5. Click on the Rule tab. Click the Add rule button then enter a name for the rule. Select a Watch list you previously configured.

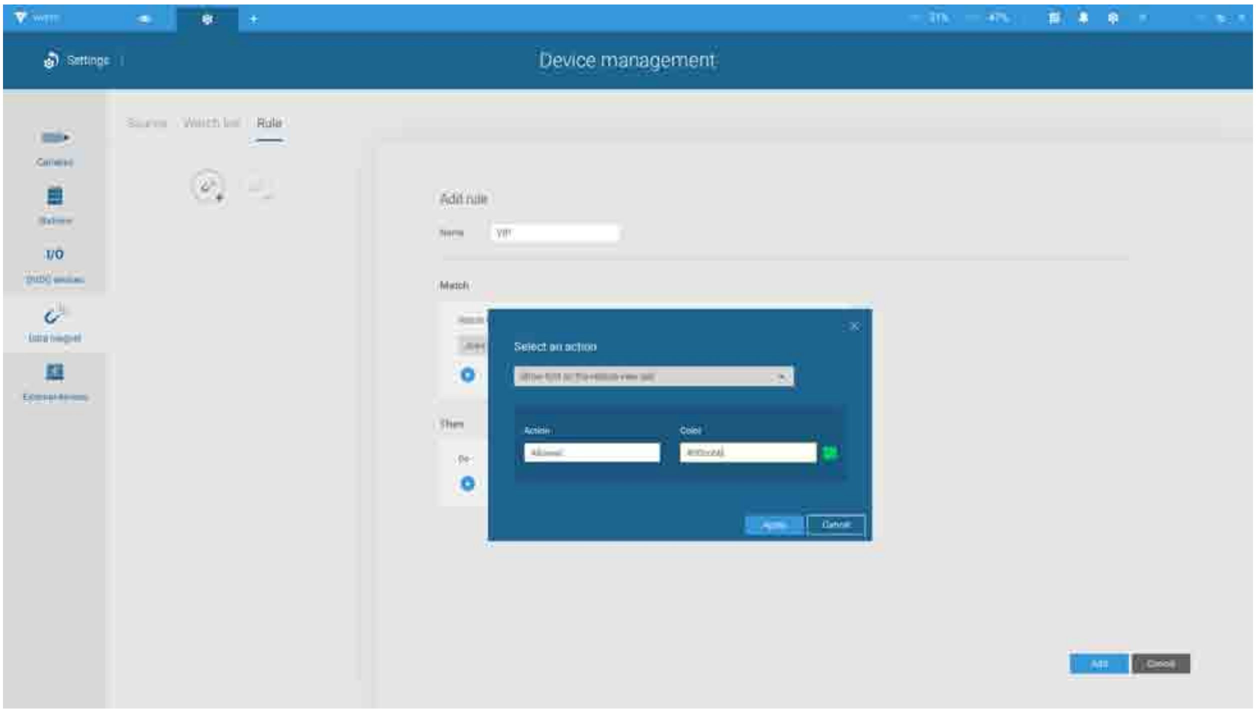


Name VIP

6. Select an action such as Show hint on the related view cell.

Enter a word you want to show on the related view cell. Enter hex color code for the word displayed on view cell. Click Add to finish the configuration.

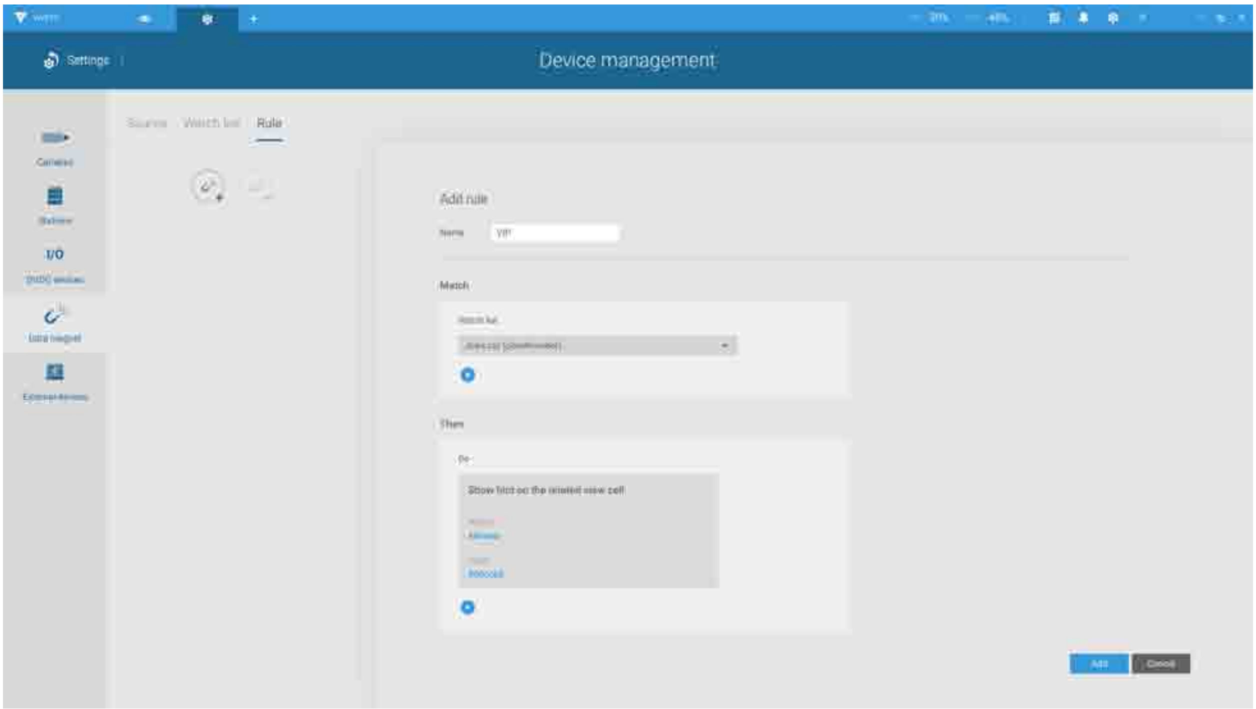
.



Name VIP

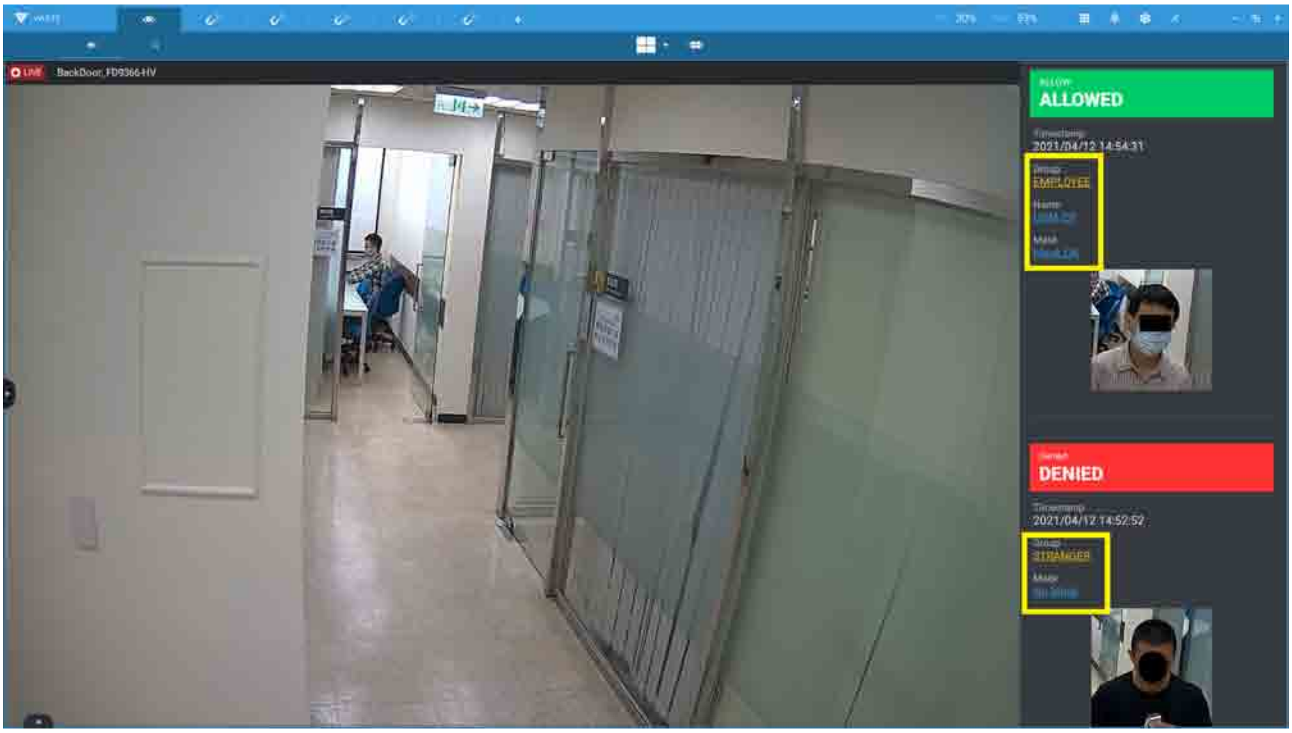
Action Allowed

Color [illegible]

Settings
Device management
Cameras
I/O
Source
Watch list
Rule
Add rule
Match
Then
Add
Cancel

Name: VIP

7. On the VAST view cell, the ALLOWED or DENIED rule message will display along with your watch list and other information.



[redacted]

[redacted]

Allow
ALLOWED

Timestamp
2021/04/12 14:54:31

Group
EMPLOYEE

Name
ODM-29

Mask
Mask OK

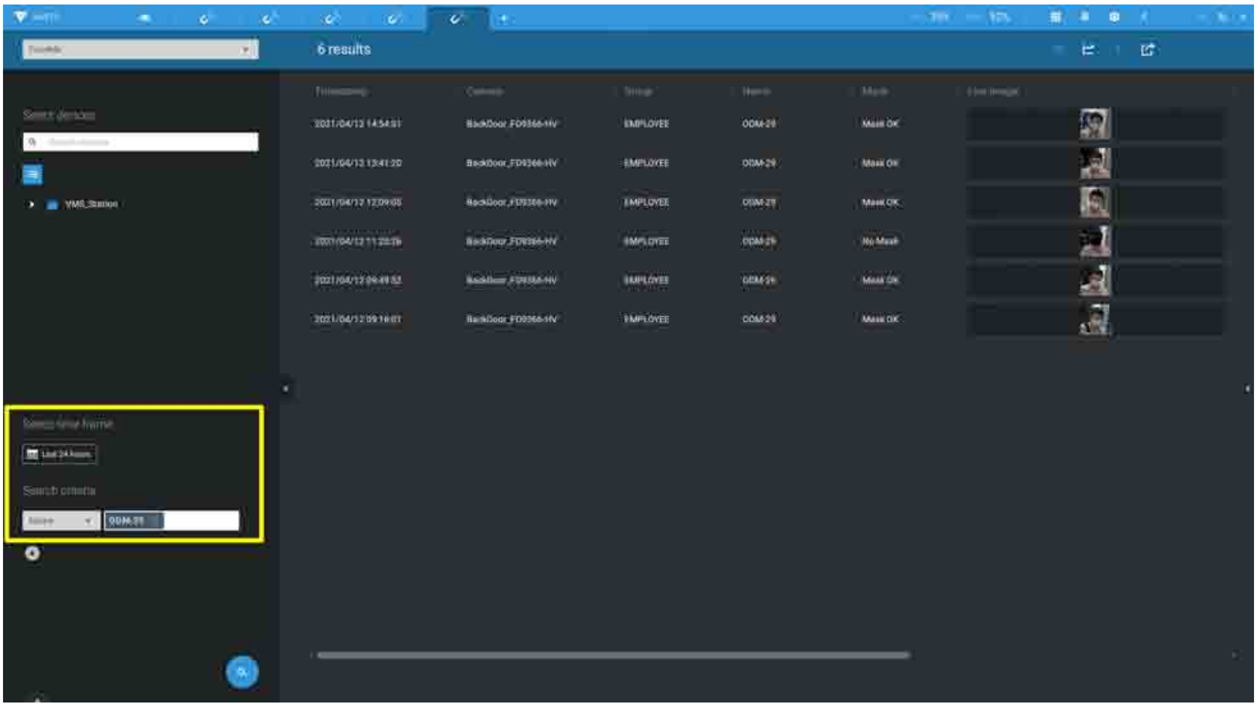
Denied
DENIED

Timestamp
2021/04/12 14:52:52

Group
STRANGER

Mask
No Mask

Since revision 2.11, you can click on the data pane to reveal a list of access occurrences matching the current circumstances. A list of similar occurrences happened within the past 24 hours will be listed.



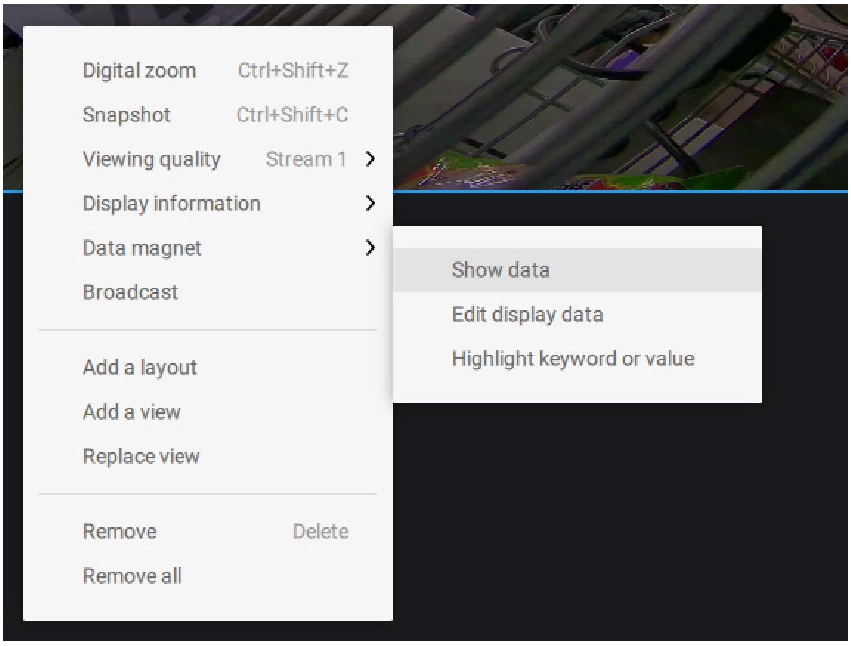
6 results

Timestamp	Camera	Group	Name	Mask	Live image
2021/04/12 14:54:31	BackDoor_FD9366-HV	EMPLOYEE	ODM-29	Mask OK	
2021/04/12 13:41:20	BackDoor_FD9366-HV	EMPLOYEE	ODM-29	Mask OK	
2021/04/12 12:09:05	BackDoor_FD9366-HV	EMPLOYEE	ODM-29	Mask OK	
2021/04/12 11:22:26	BackDoor_FD9366-HV	EMPLOYEE	ODM-29	No Mask	
2021/04/12 09:49:52	BackDoor_FD9366-HV	EMPLOYEE	ODM-29	Mask OK	
2021/04/12 09:16:01	BackDoor_FD9366-HV	EMPLOYEE	ODM-29	Mask OK	

Selecting data display options:

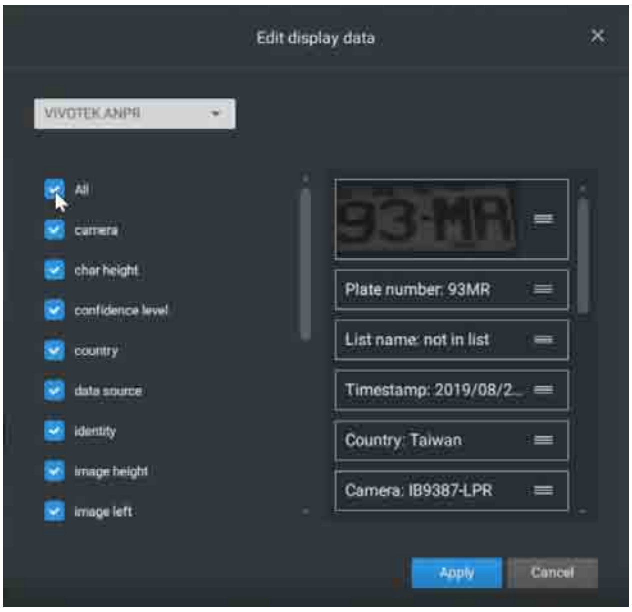
1. On the VAST live view, right-click on screen to display Data Magnet > **Edit display data**. If **Show data** is selected, a portion of the view cell will be used to display the captured data.

   There are two different ways to show data:
   1. Right-click: Data Magnet > Show data.
   2. Right-click: Display information > Edit display information > Data magnet data.
   The display options are: with or without Data overlay on screen. If the overlay is not enabled, the data will display on the right pane of the view cell.



The data on the overlay can be configured to automatically disappear after a configurable time, when no new data is received (Hide data after idle _ s).

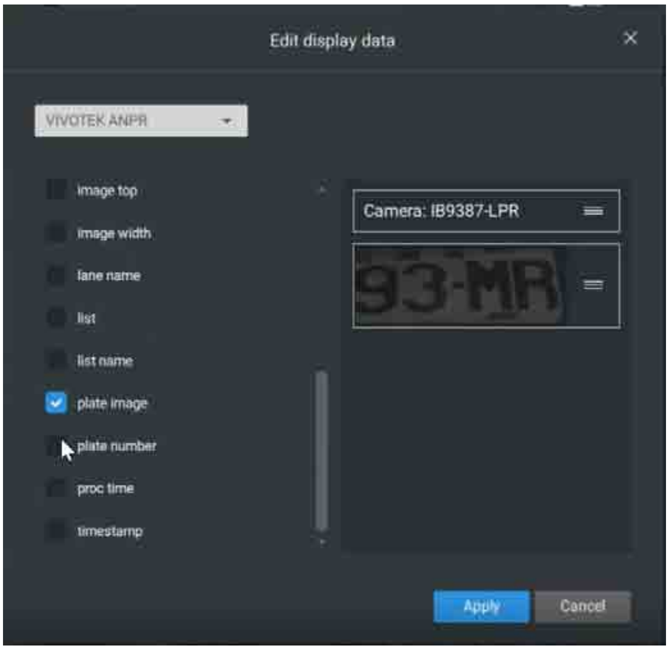
2. On the Edit pane, select all or manually select multiple display elements.


Edit display data

VIVOTEK ANPR

☑ All
☑ camera
☑ char height
☑ confidence level
☑ country
☑ data source
☑ identity
☑ image height
☑ image left

Plate number: 93MR
List name: not in list
Timestamp: 2019/08/2...
Country: Taiwan
Camera: IB9387-LPR

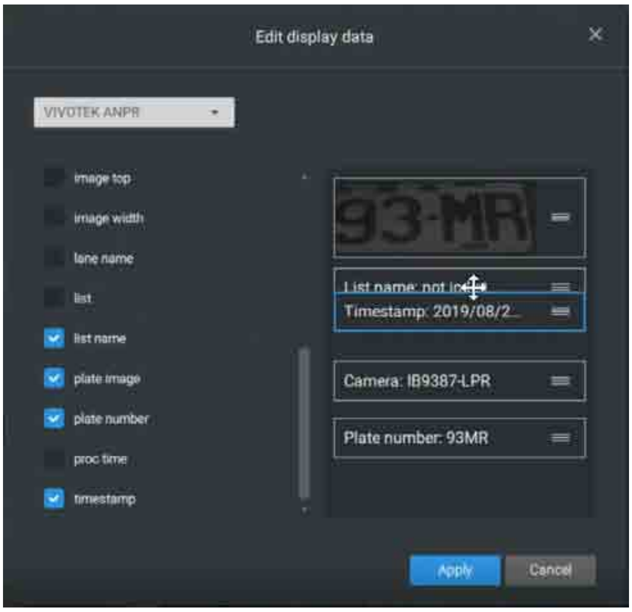

Edit display data

VIVOTEK ANPR

□ image top
□ image width
□ lane name
□ list
□ list name
☑ plate image
□ plate number
□ proc time
□ timestamp

Camera: IB9387-LPR

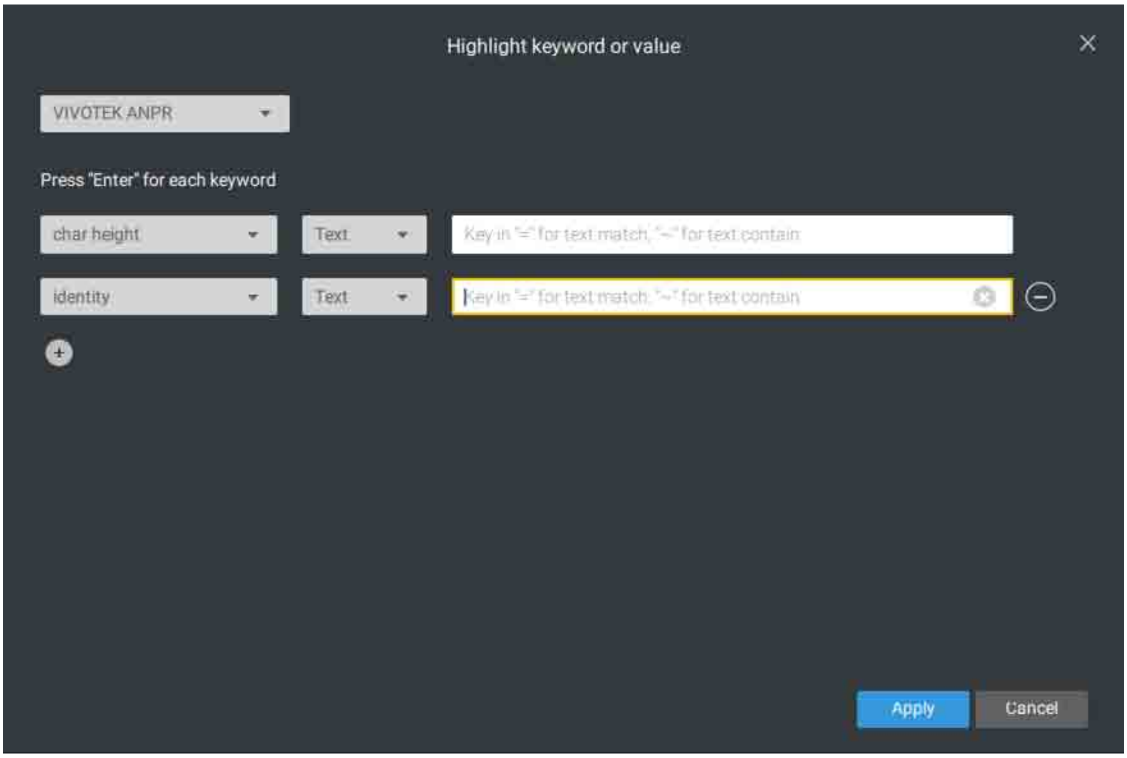
3. Click and drag individual elements to change their top-down positions on the screen. When done, click the **Apply** button.



□ image top
□ image width
□ lane name
□ list
☑ list name
☑ plate image
☑ plate number
□ proc time
☑ timestamp

List name: not in...
Timestamp: 2019/08/2...
Camera: IB9387-LPR
Plate number: 93MR

4. Click **Highlight keyword or value**. You can display information of unusual data, such as the specific numbers or characters of forbidden license plates. When such data is met, the occurrence will be highlighted in a bright yellow color.



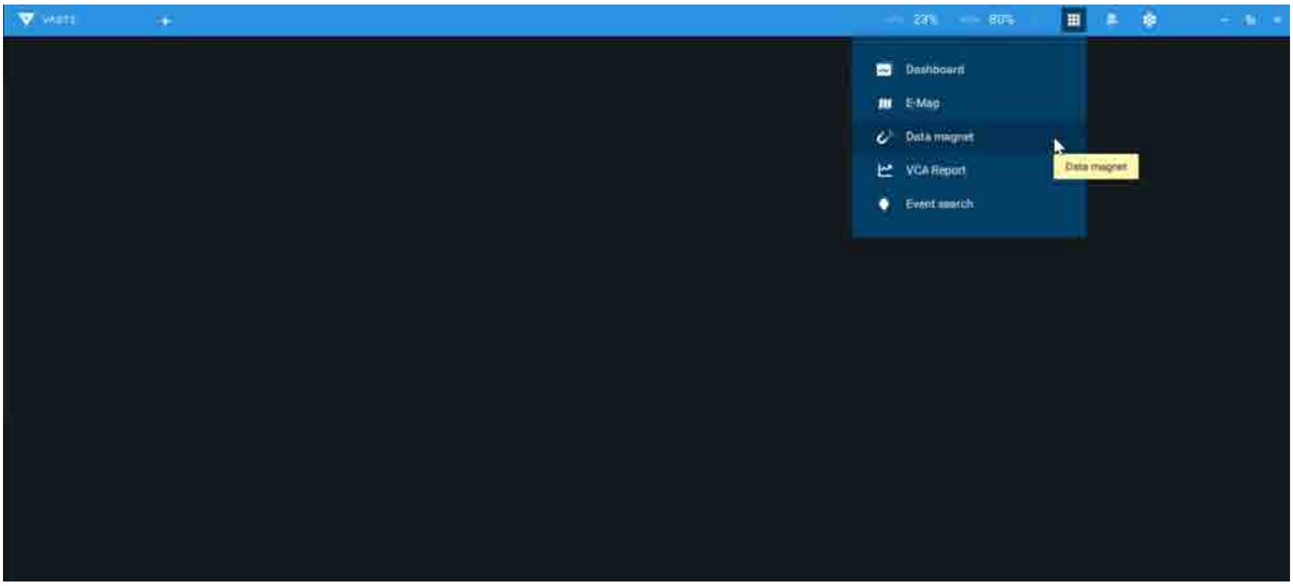
Press "Enter" for each keyword

char height | Text | Key in "=" for text match, "~" for text contain

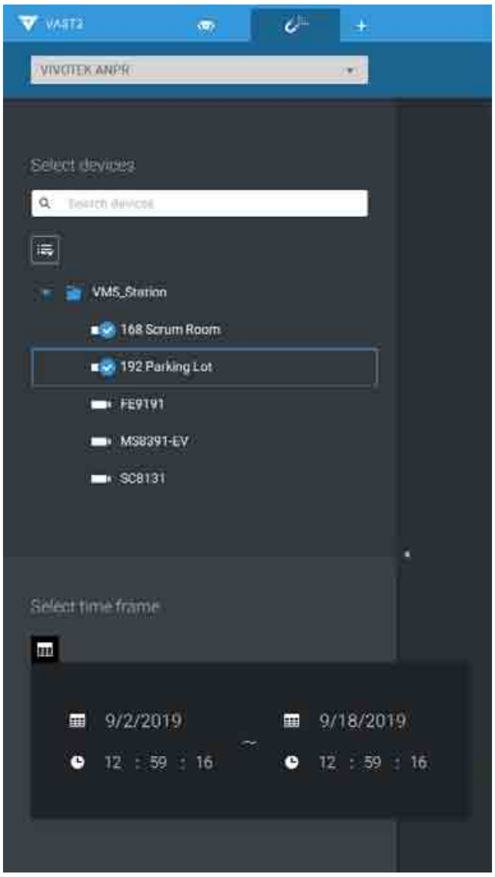
identity | Text | Key in "=" for text match, "~" for text contain

Searching for data and linked recordings:

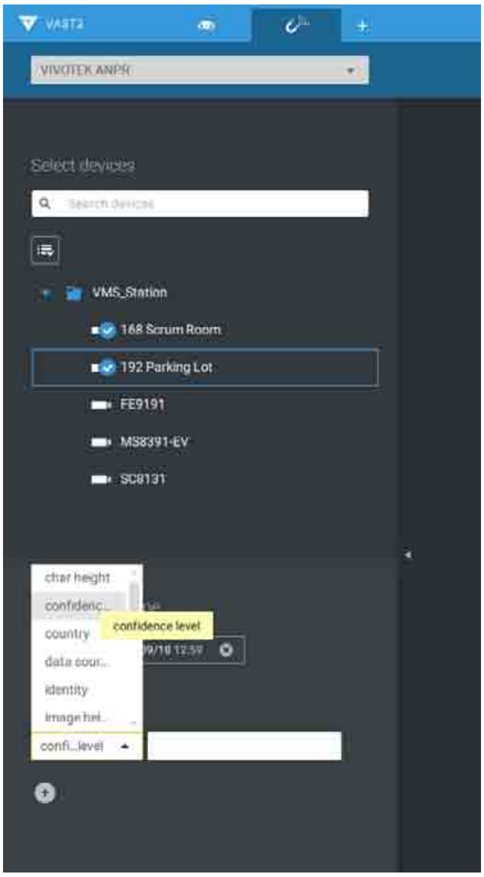
1. On the VAST live view, click on the Applications tab.



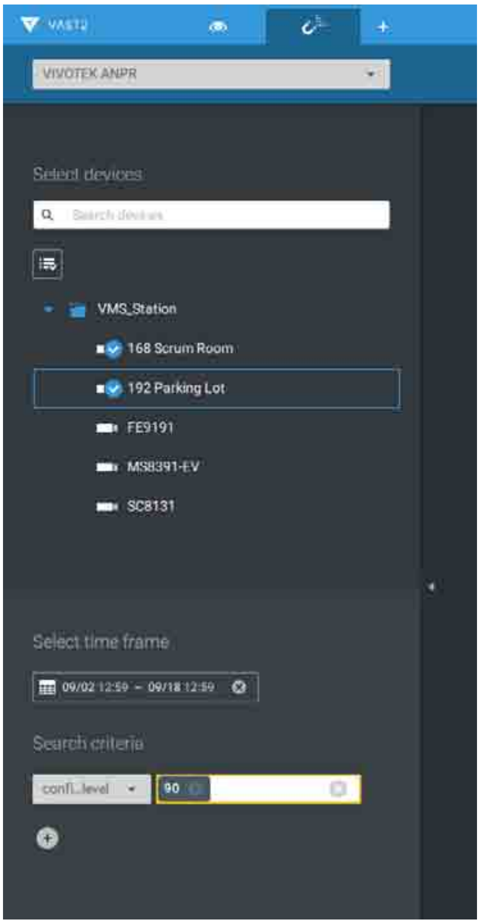
2. On the Data Magnet window, select the LPR camera, and then begin with configuring the search conditions. Select the time span from the calendar. Select to display character height, country, data source, identity, image height, lane name, list name, or enter a plate number. You can select multiple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



9/2/2019 12 : 59 : 16 ~ 9/18/2019 12 : 59 : 16



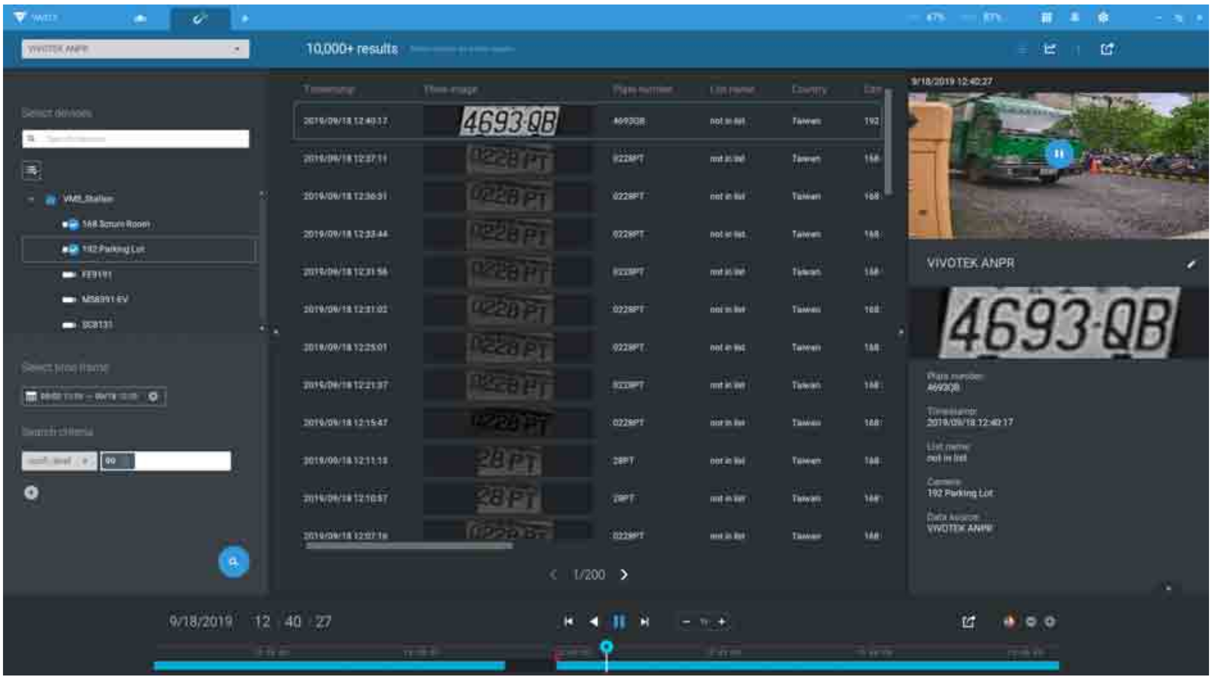
confi...level



09/02 12:59 ~ 09/18 12:59

confi...level 90

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.



10,000+ results

Timestamp	Plate image	Plate number	List name	Country	Cam
2019/09/18 12:40:17		4693QB	not in list	Taiwan	192
2019/09/18 12:37:11		0228PT	not in list	Taiwan	168
2019/09/18 12:36:31		0228PT	not in list	Taiwan	168
2019/09/18 12:33:44		0228PT	not in list	Taiwan	168
2019/09/18 12:31:56		0228PT	not in list	Taiwan	168
2019/09/18 12:31:02		0228PT	not in list	Taiwan	168
2019/09/18 12:25:01		0228PT	not in list	Taiwan	168
2019/09/18 12:21:37		0228PT	not in list	Taiwan	168
2019/09/18 12:15:47		0228PT	not in list	Taiwan	168
2019/09/18 12:11:13		28PT	not in list	Taiwan	168
2019/09/18 12:10:57		28PT	not in list	Taiwan	168
2019/09/18 12:07:16		0228PT	not in list	Taiwan	168

9/18/2019 12:40:27

VIVOTEK ANPR

Plate number: 4693QB

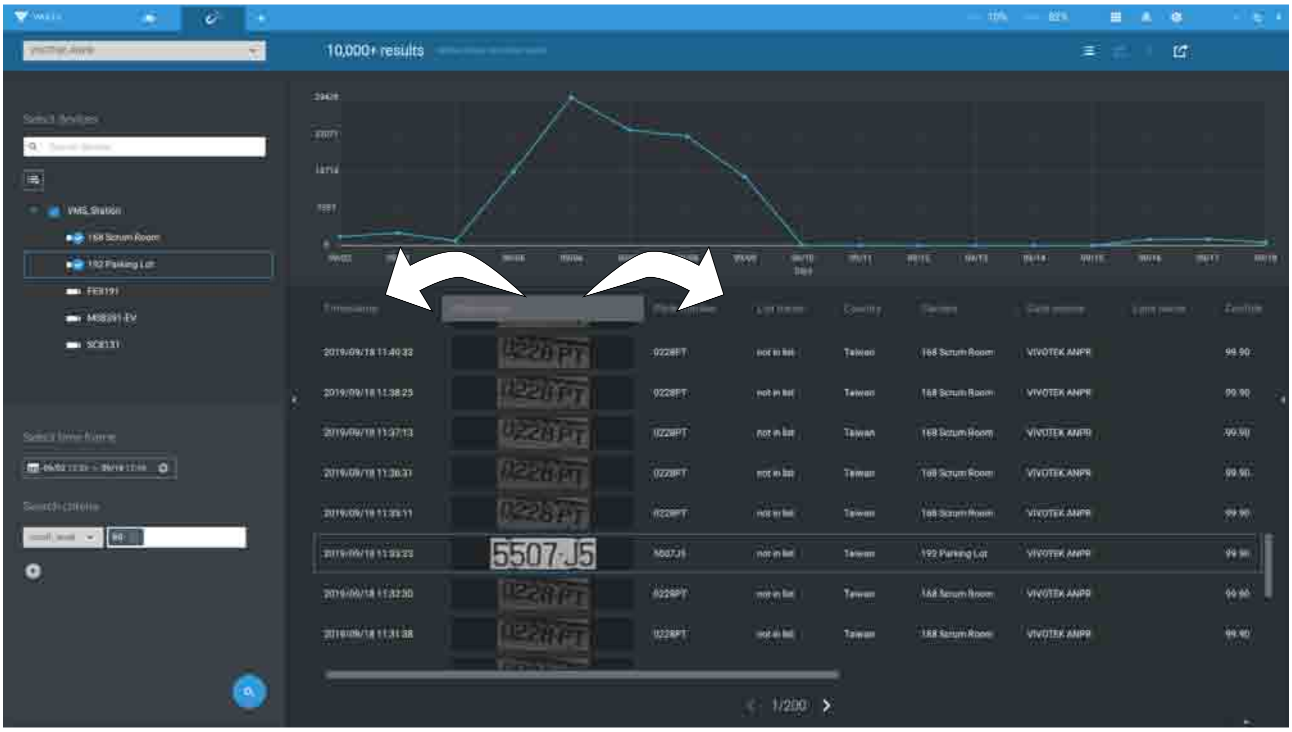
Timestamp: 2019/09/18 12:40:17

List name: not in list

Camera: 192 Parking Lot

Data source: VIVOTEK ANPR

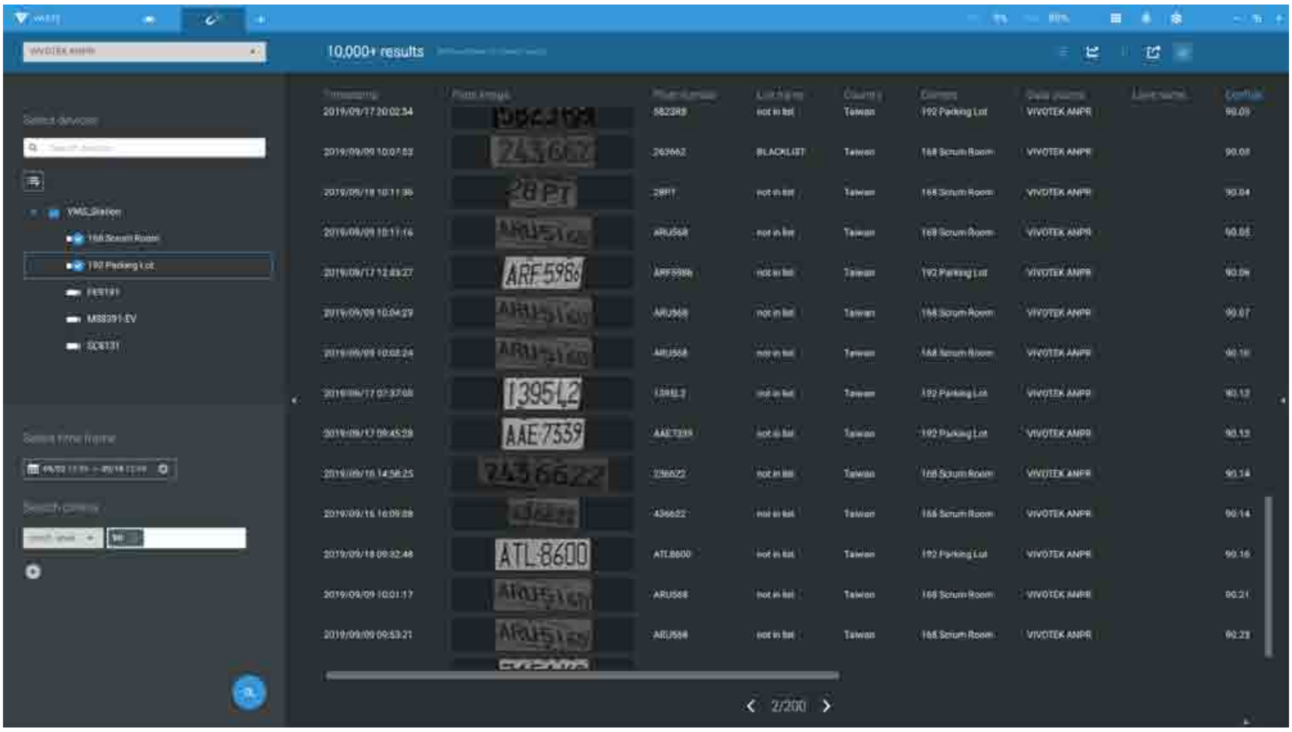
You can click and drag the display names of individual columns to switch their positions on the screen. The changes to layout are stored on the client computer. After you re-arrange the order of columns in search results, the display order will also be applied to the exported CSV file.



10,000+ results

Timestamp	Plate image	Plate number	List name	Country	Camera	Data source	Lane name	Confidence
2019/09/18 11:40:32		0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
2019/09/18 11:38:25		0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
2019/09/18 11:37:13		0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
2019/09/18 11:36:31		0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
2019/09/18 11:35:11		0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
2019/09/18 11:33:23		5507J5	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR		99.90
2019/09/18 11:32:30		0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90
2019/09/18 11:31:38		0228PT	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		99.90

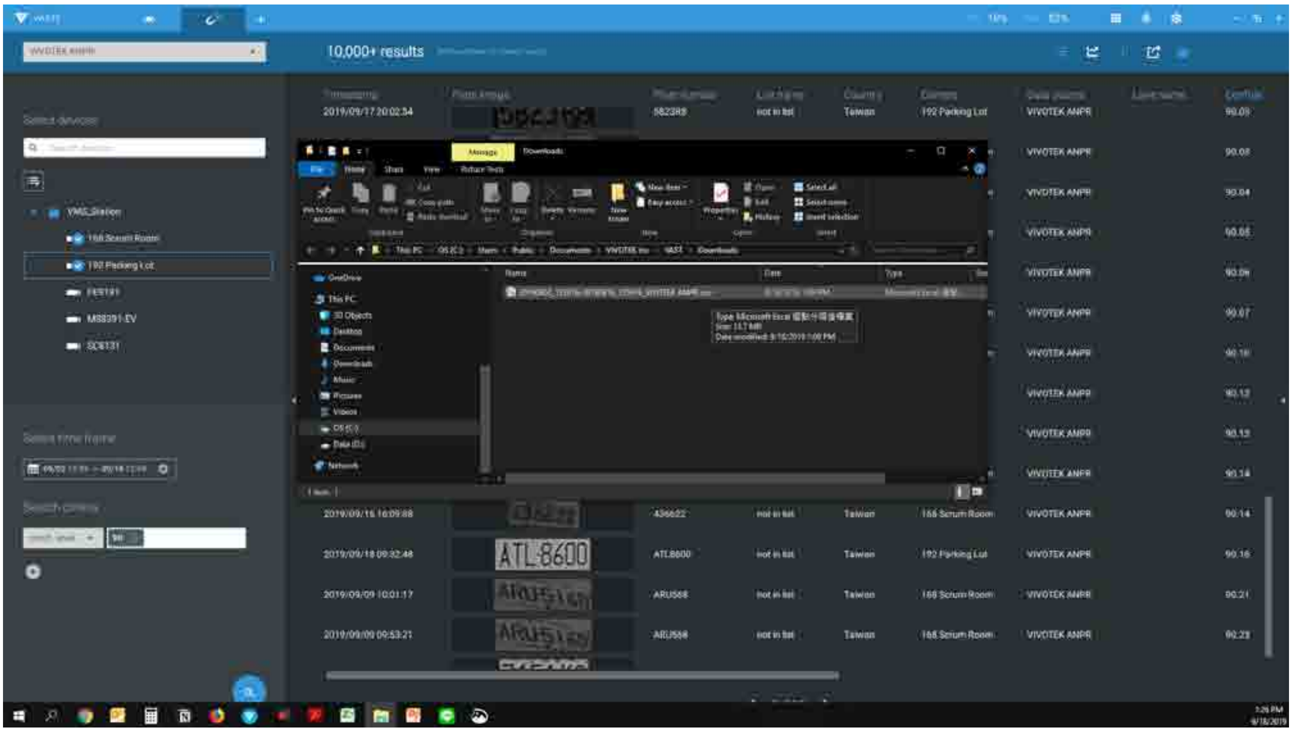
4. You can select and export a license plate capture using the Export function. Click on the export button. A folder button will display. Click on it to access the exported file.



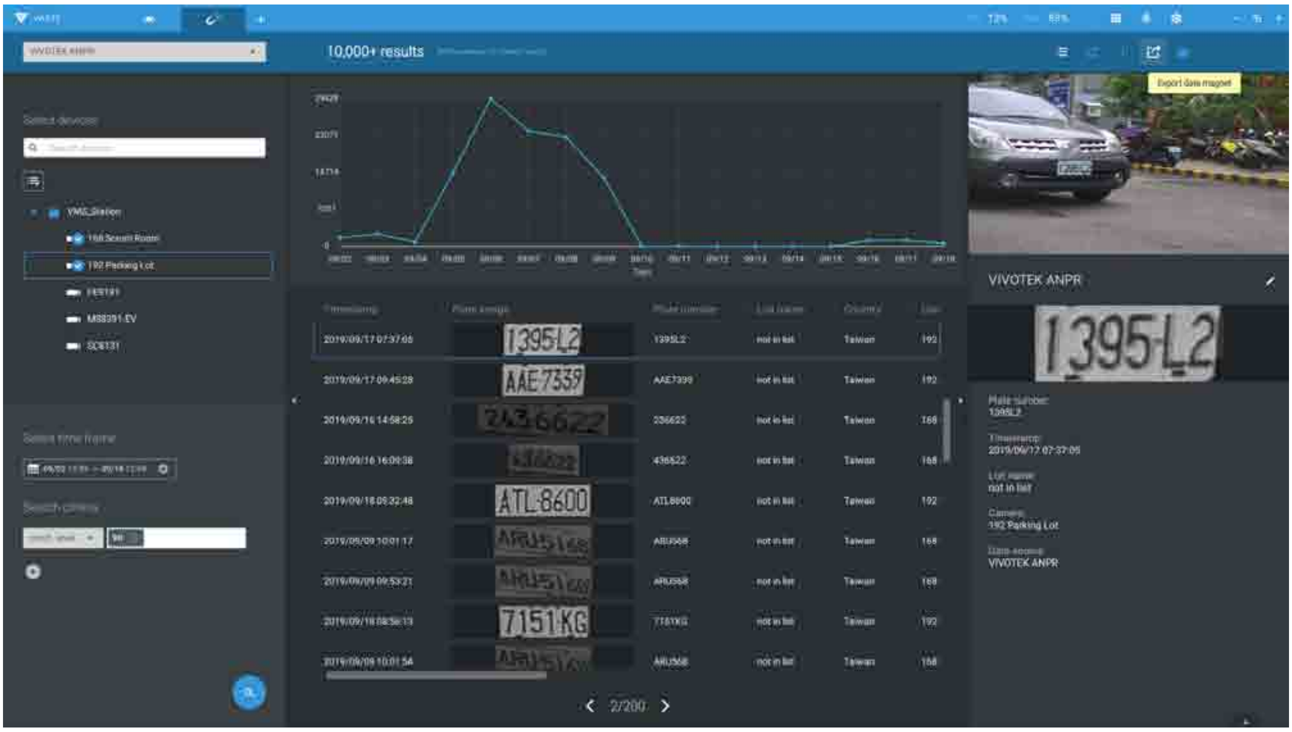
10,000+ results

Timestamp	Plate image	Plate number	List name	Country	Camera	Data source	Lane name	Confidence
2019/09/17 20:02:34		5823R9	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR		90.09
2019/09/09 10:07:53		263662	BLACKLIST	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.03
2019/09/18 10:11:36		28P1	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.04
2019/09/09 10:11:16		ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.05
2019/09/17 12:43:27		ARF5986	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR		90.06
2019/09/09 10:04:29		ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.07
2019/09/09 10:02:24		ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.10
2019/09/17 07:37:08		1395L2	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR		90.12
2019/09/17 09:45:28		AAE7339	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR		90.13
2019/09/16 14:58:25		236622	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.14
2019/09/16 16:09:08		436622	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.14
2019/09/18 09:32:48		ATL8600	not in list	Taiwan	192 Parking Lot	VIVOTEK ANPR		90.16
2019/09/09 10:01:17		ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.21
2019/09/09 09:53:21		ARU568	not in list	Taiwan	168 Scrum Room	VIVOTEK ANPR		90.23

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.



Timestamp	Plate image	Plate number	List name	Country	Lan
2019/09/17 07:37:05	1395L2	1395L2	not in list	Taiwan	192
2019/09/17 09:45:28	AAE7339	AAE7399	not in list	Taiwan	192
2019/09/16 14:58:25	2A3 6622	236622	not in list	Taiwan	168
2019/09/16 16:09:38	[illegible]	436622	not in list	Taiwan	168
2019/09/18 09:32:48	ATL-8600	ATL8600	not in list	Taiwan	192
2019/09/09 10:01:17	[illegible]	ARU568	not in list	Taiwan	168
2019/09/09 09:53:21	[illegible]	ARU568	not in list	Taiwan	168
2019/09/18 08:56:13	7151KG	7151KG	not in list	Taiwan	192
2019/09/09 10:01:54	[illegible]	ARU568	not in list	Taiwan	168

2/200

VIVOTEK ANPR

Plate number: 1395L2

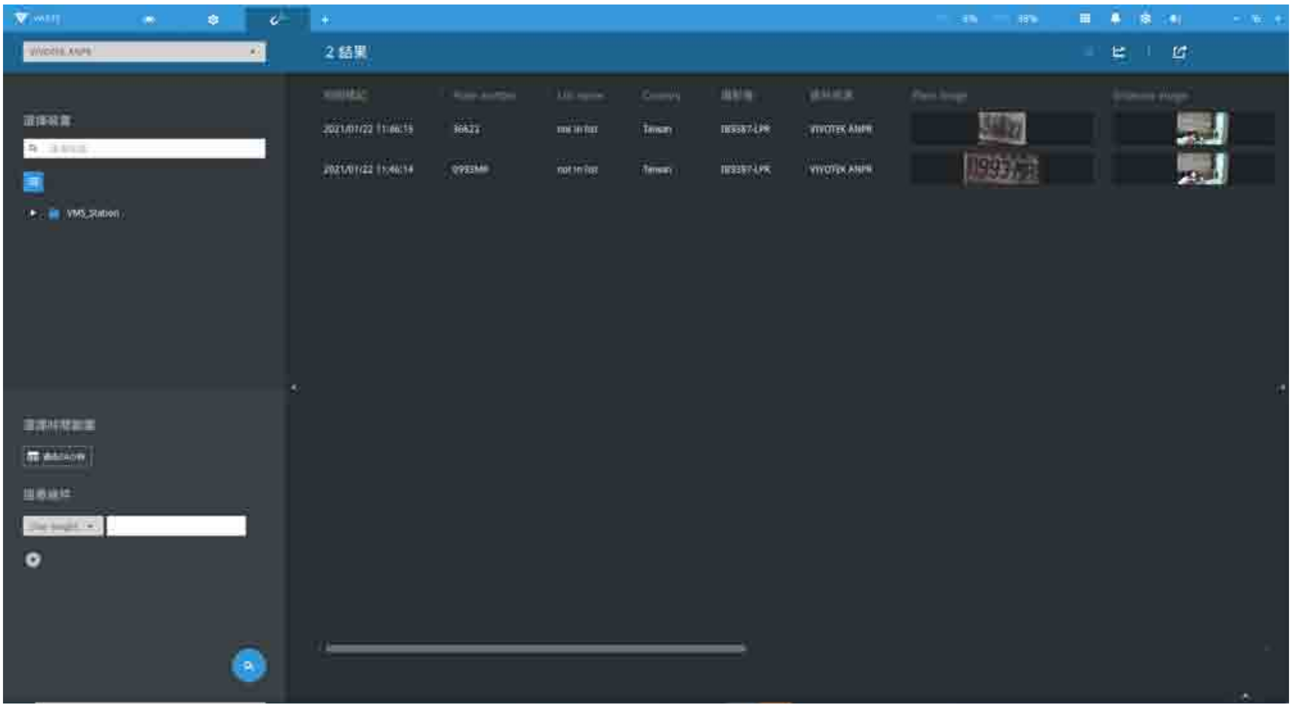
Timestamp: 2019/09/17 07:37:05

List name: not in list

Camera: 192 Parking Lot

Data source: VIVOTEK ANPR

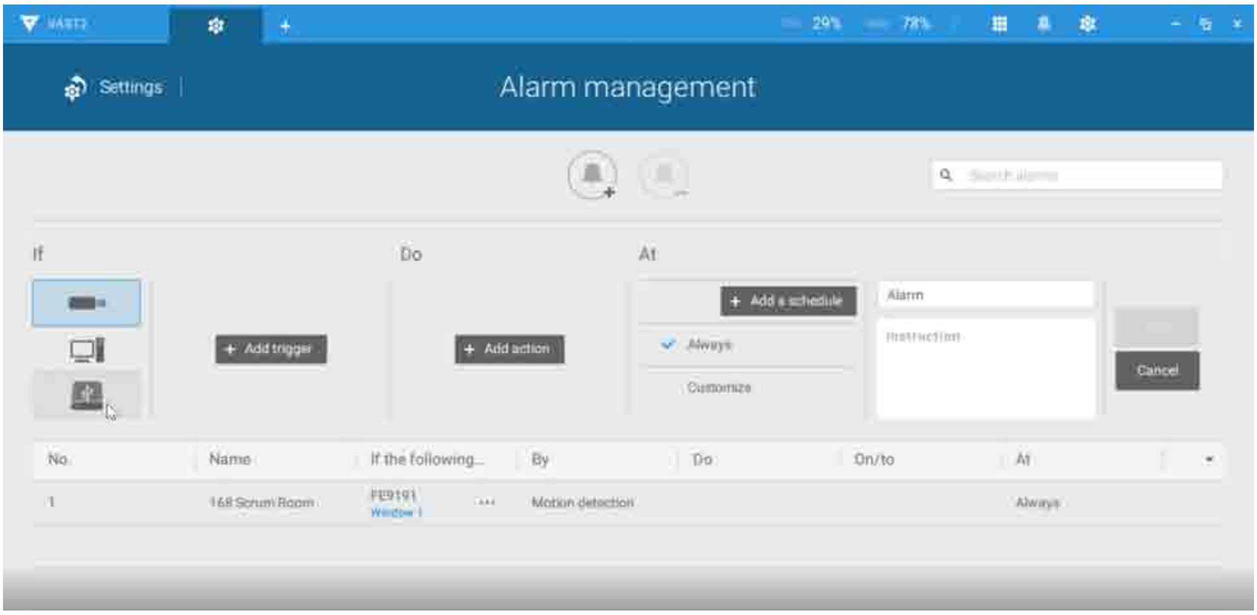
On VAST rev. 2.10, an evidence image will be available with the search result along with the plate picture.



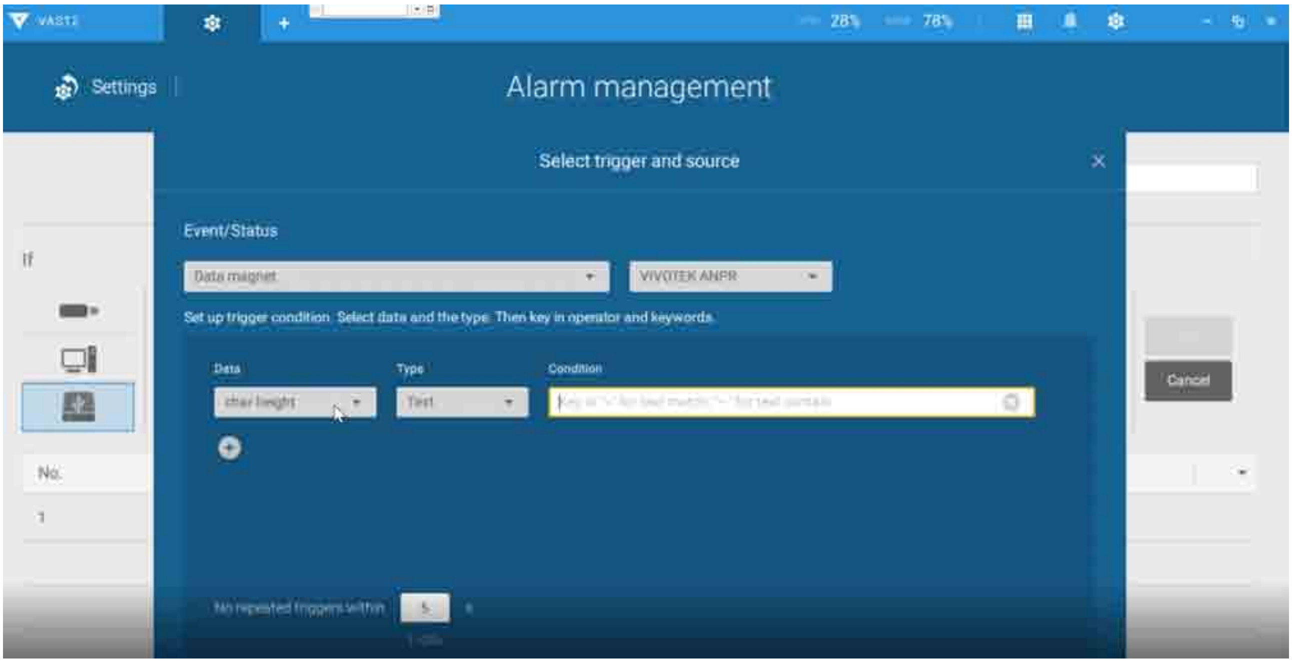
[illegible]	Plate number	List name	Country	攝影機	資料來源	Plate image	Evidence image
2021/01/22 11:46:15	36621	not in list	Taiwan	IB9387-LPR	VIVOTEK ANPR		
2021/01/22 11:46:14	0993MP	not in list	Taiwan	IB9387-LPR	VIVOTEK ANPR		

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.



Select trigger and source

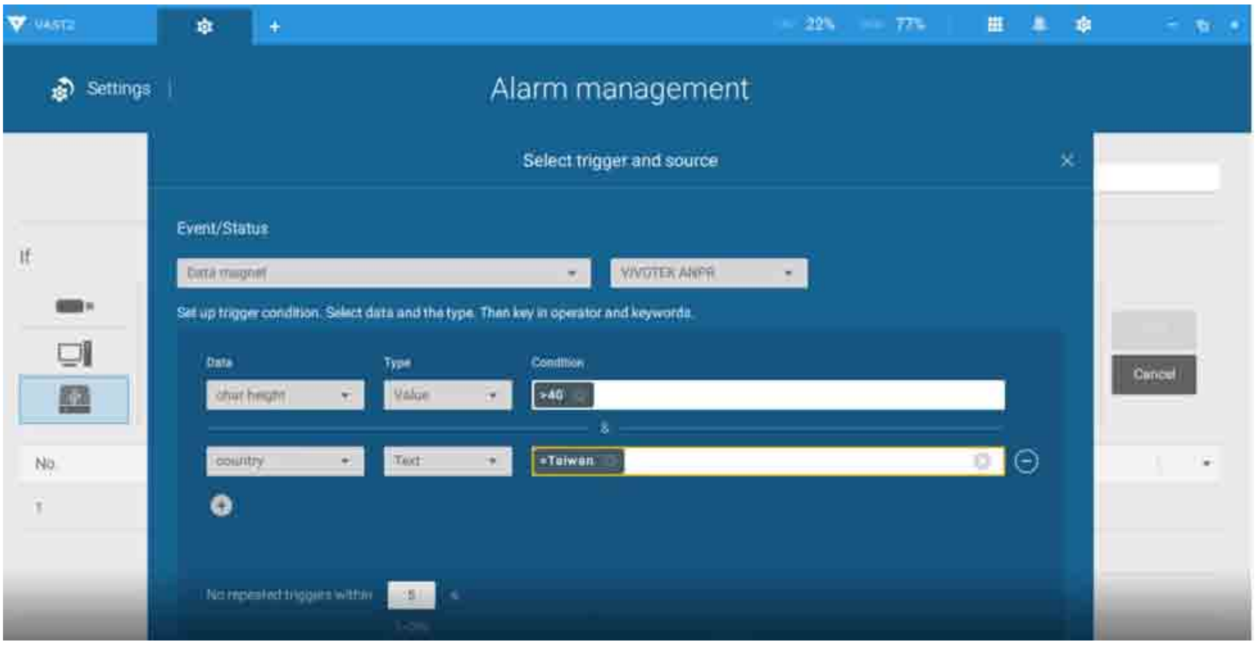
Event/Status: Data magnet | VIVOTEK ANPR

Set up trigger condition. Select data and the type. Then key in operator and keywords.

Data	Type	Condition
char height	Text	Key in "=" for text match, "~" for text contain

No repeated triggers within 5 s

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



Select trigger and source

Event/Status

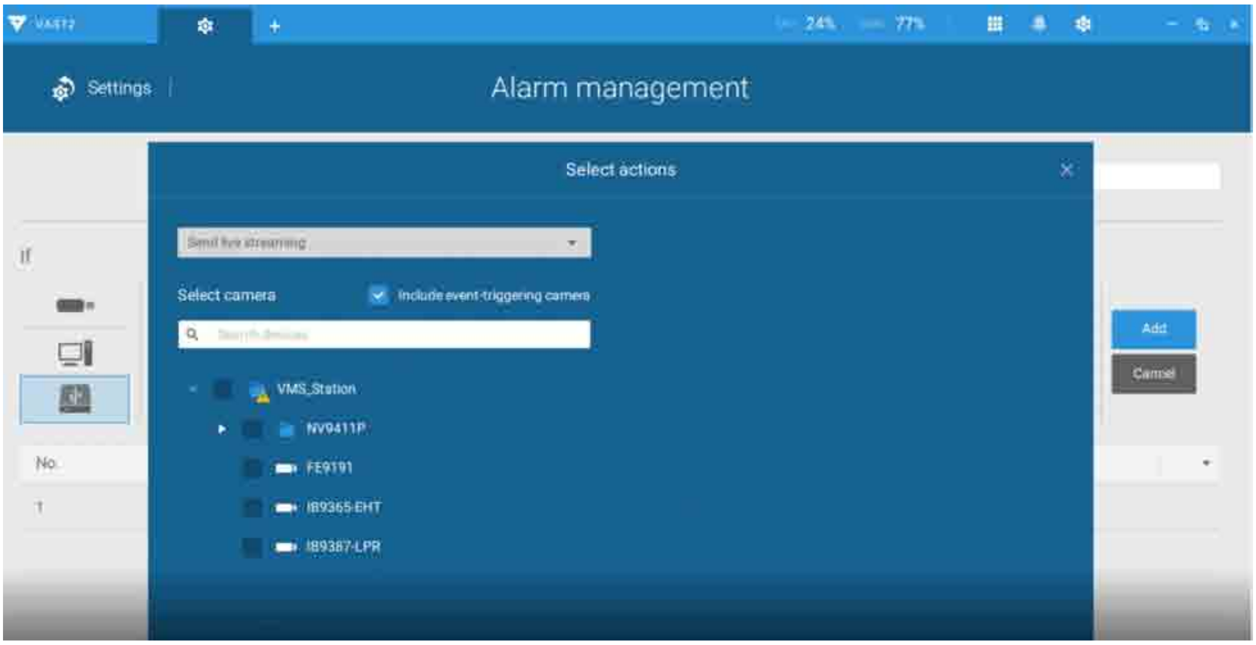
Data magnet ▾ | VIVOTEK ANPR ▾

Set up trigger condition. Select data and the type. Then key in operator and keywords.

Data	Type	Condition
char height	Value	>40
country	Text	=Taiwan

No repeated triggers within 5 s

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



Select actions

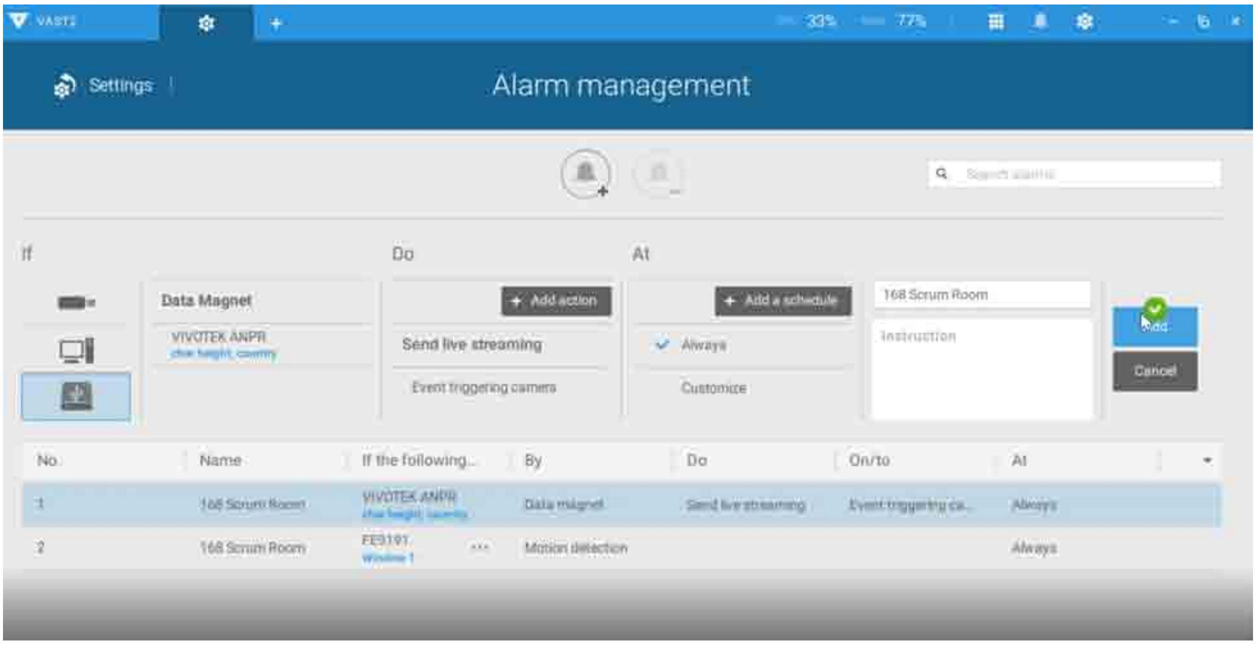
Send live streaming ▾

Select camera ☑ Include event-triggering camera

Search devices

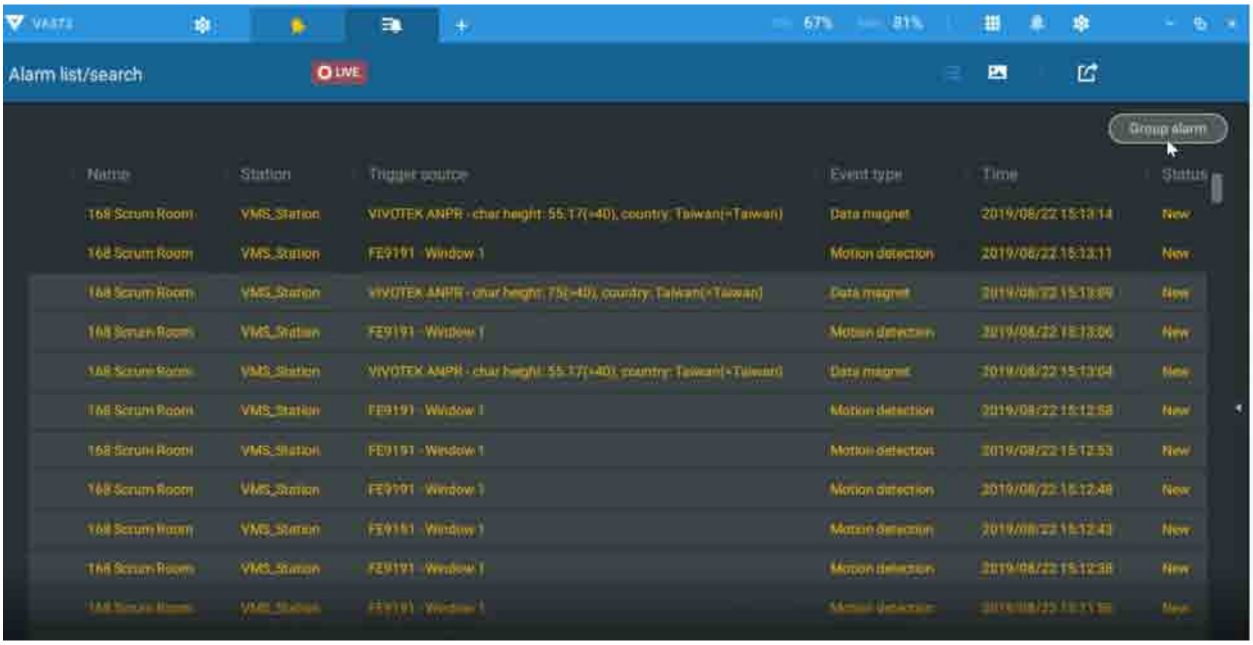
- VMS_Station
  - NV9411P
  - FE9191
  - IB9365-EHT
  - IB9387-LPR

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



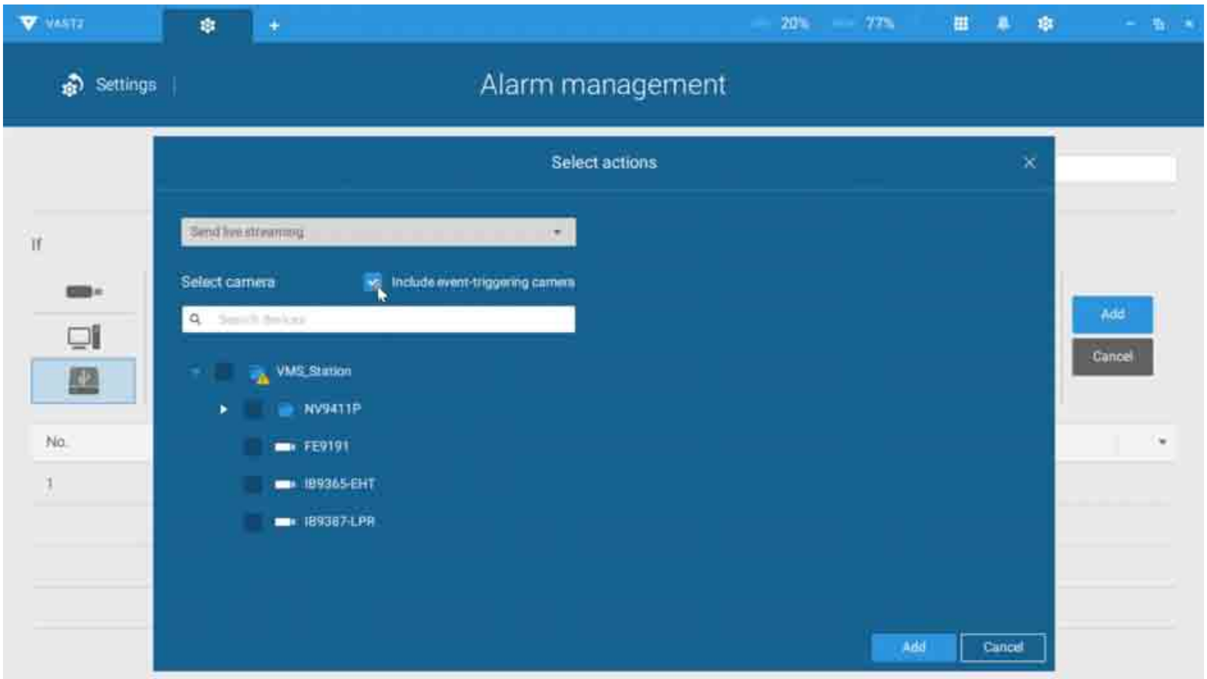
No.	Name	If the following...	By	Do	On/to	At
1	168 Scrum Room	VIVOTEK ANPR char height, country	Data magnet	Send live streaming	Event triggering ca...	Always
2	168 Scrum Room	FE9191 Window 1	Motion detection			Always

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



Name	Station	Trigger source	Event type	Time	Status
168 Scrum Room	VMS_Station	VIVOTEK ANPR - char height: 55.17(<40), country: Taiwan(=Taiwan)	Data magnet	2019/08/22 15:13:14	New
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/08/22 15:13:11	New
168 Scrum Room	VMS_Station	VIVOTEK ANPR - char height: 75(<40), country: Taiwan(=Taiwan)	Data magnet	2019/08/22 15:13:09	New
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/08/22 15:13:06	New
168 Scrum Room	VMS_Station	VIVOTEK ANPR - char height: 55.17(<40), country: Taiwan(=Taiwan)	Data magnet	2019/08/22 15:13:04	New
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/08/22 15:12:58	New
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/08/22 15:12:53	New
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/08/22 15:12:48	New
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/08/22 15:12:43	New
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	2019/08/22 15:12:38	New
168 Scrum Room	VMS_Station	FE9191 - Window 1	Motion detection	[illegible]	New

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

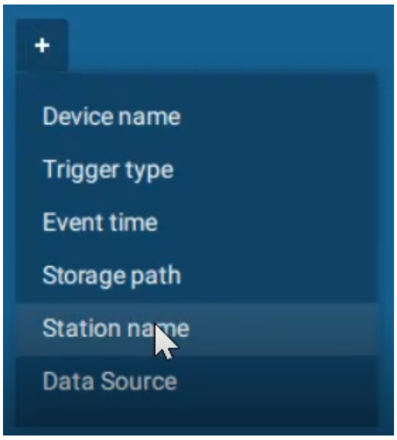


Send live streaming

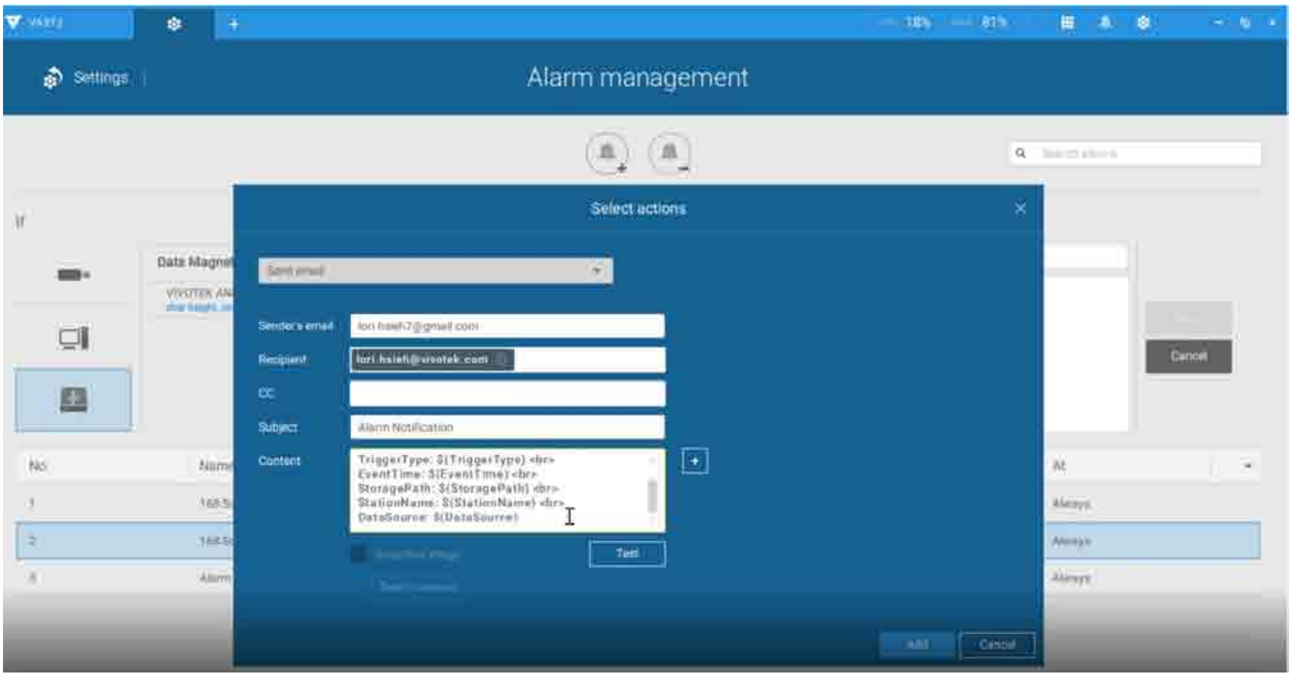
☑ Include event-triggering camera

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 "<br>" 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.



Sender's email: lori.hsieh7@gmail.com

Recipient: lori.hsieh@vivotek.com

CC:

Subject: Alarm Notification

Content:

```
TriggerType: $(TriggerType) <br>
EventTime: $(EventTime) <br>
StoragePath: $(StoragePath) <br>
StationName: $(StationName) <br>
DataSource: $(DataSource)
```

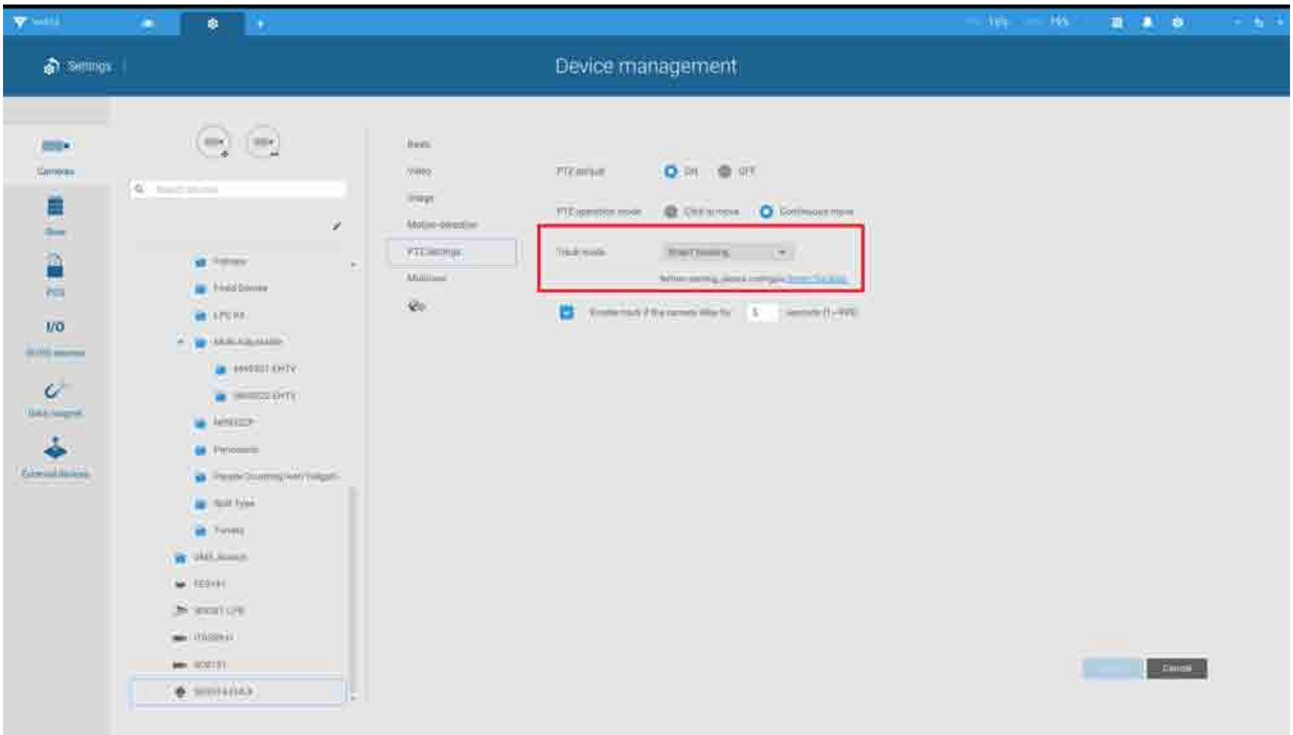
Appendix H: Enable Smart Tracking for Speed Dome Cameras

The Smart tracking function is available on speed dome cameras, such as SD9374-EHLX. The Smart tracking feature is separately configured on the camera side. Please refer to Smart Tracking User Guide for configuration details.

To display Smart tracking on VAST,

1. Enter Settings > Devices > Cameras.
2. Select the speed dome camera that supports this feature.
3. Select PTZ Settings, and the Track mode menu. Select **Smart tracking** as the tracking display mode. A hyperlink is provided for the Smart tracking configuration page.

   It is recommended to always enable "Enable track if the camera idles for xx seconds." Manual PTZ control always has a higher priority and will interrupt tracking.
4. Click the **Apply** button.



PTZ output ● On ○ OFF

PTZ operation mode ○ Click to move ● Continuous move

Track mode Smart tracking

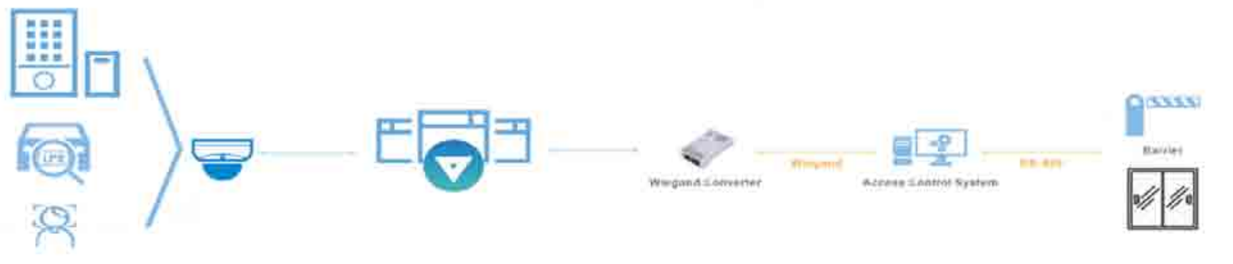
☑ Enable track if the camera idles for 5 seconds (1~999)

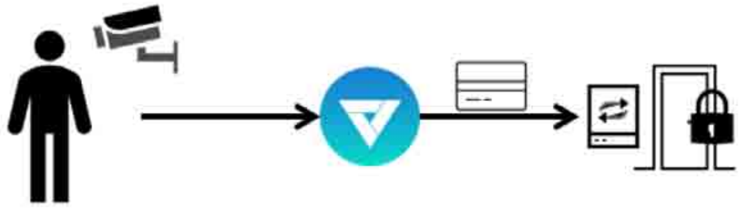
Appendix I: Multi-factor Authentication for Access Control

Via multiple data magnet sources, access authentication can be achieved for the following: 1. License plate recognition system, Face recognition system, 3. Access control system.

For example, in a parking lot, if someone wants to leave, the LPR system at the gate will recognize the license plate, and the face recognition will verify the driver's identity. If both recognition succeed, the gate will open allowing the driver to leave.

In an office, an access control system can be combined with Face recognition mechanism to avoid someone using someone else' card to cheat the attendance system.

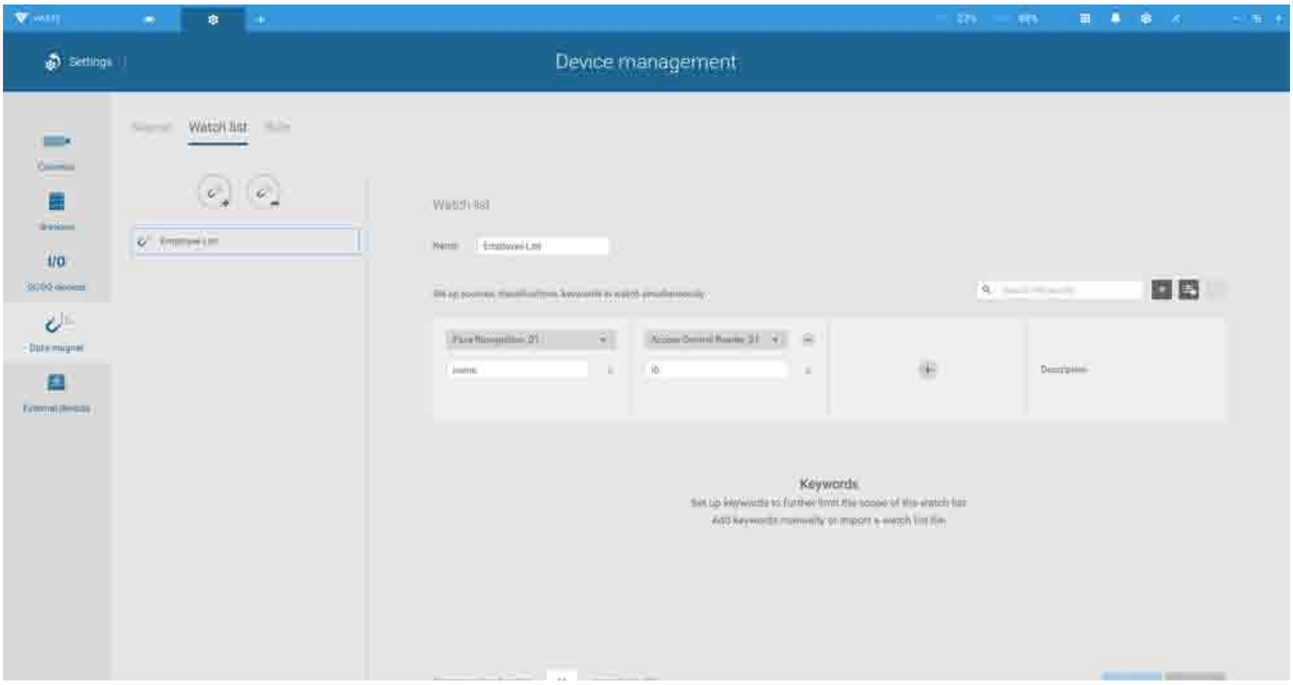




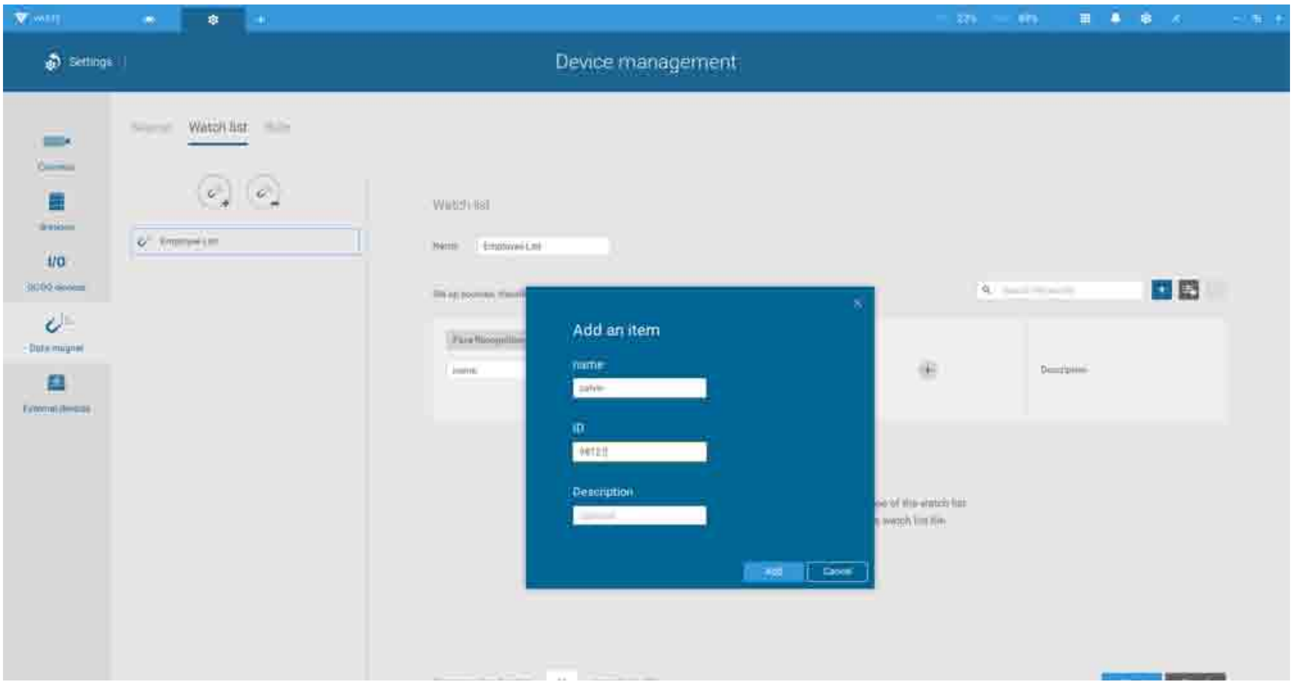
The scenario shows one holds an ID card and via the Face recognition system, his identity is verified as one employee in the database. VAST2 then acquires his ID card serial no., passes it on to an Wiegand converter. The Wiegand converter then passes it to the access control. In addition to the original ID card access control, multiple utilities can be combined into the access control mechanism.

To acquire data from multi-factor systems, we use the Watch list on Data Magnet.

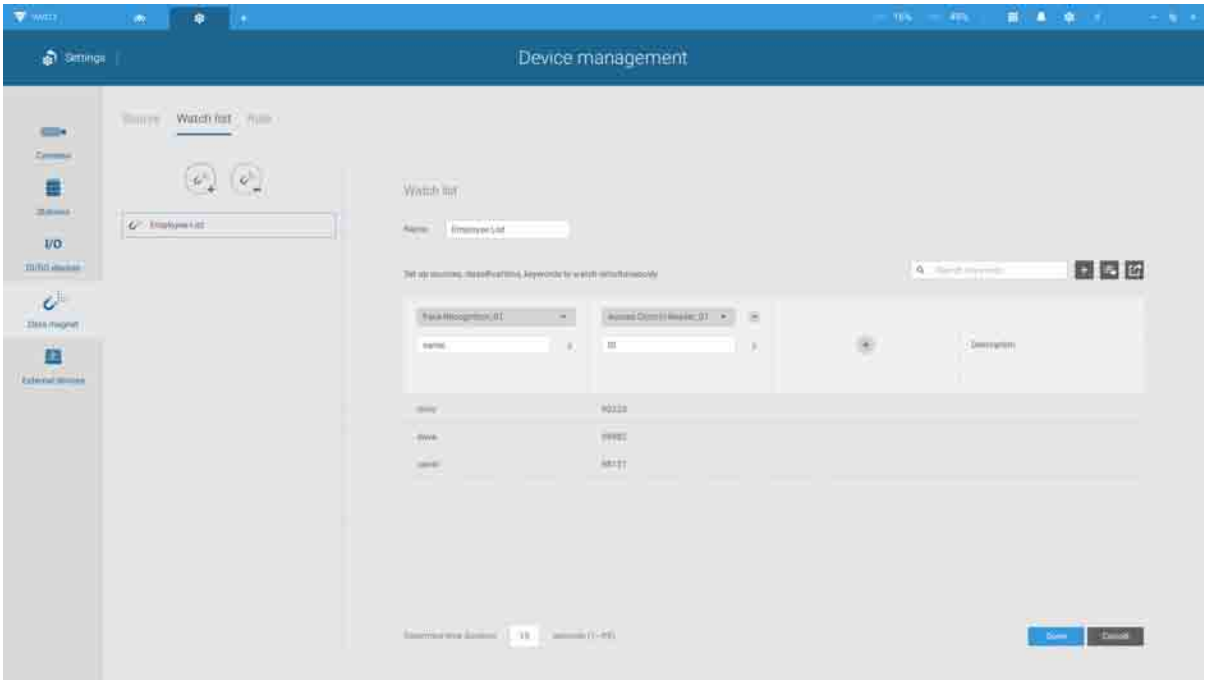
1. Depending on your applications, configure mutiple data magnet sources, so that data can be transferred and acquired by VAST.
2. Click and select Watch list in the Data Magnet window. Click the Add watch list button, and enter a name, e.g., Employee list. Select 2 or 3 pre-configured data sources, and enter the classification you would like to watch for the referential parameter in your Data Magnet json, e.g., name, ID.



3. Click the Add item button and enter a name and employee ID such as one for an employee. Click Add to finish, and repeat the process for more items.

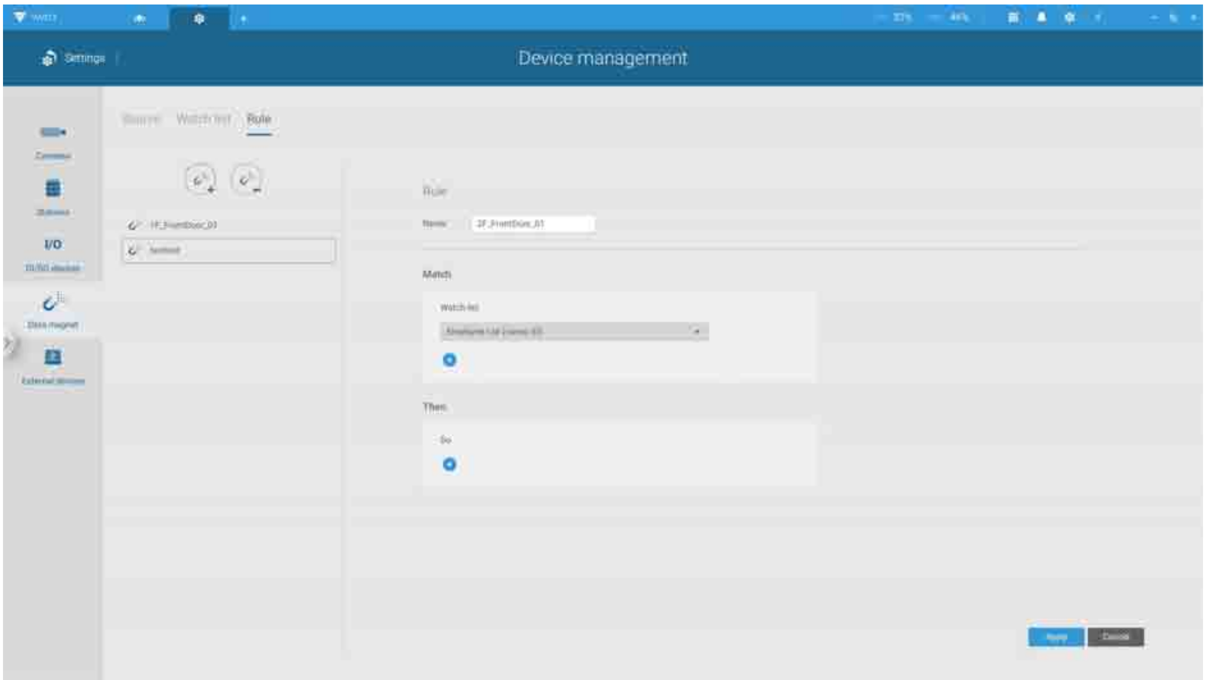


4. At the lower screen, enter the time threshold for receiving data from multiple sources. For example, If set to 15 seconds, VAST will need to receive within this time the facial recognition and the card ID no. from the access control reader. Both data will be verified and checked against the data on the watch list, e.g., name=Chris, ID=90223.



5. Click on the Rule tab. Click the Add rule button, and then enter a name for the rule. In the Match block, select a Watch list you previously configured. In the Then field, you can configure your rule action. There are 2 actions available:
   1. Show hint on the related view cell. 2. Select data to send to Wiegand converter.

   If you apply your rule to be an alarm management trigger, you can bypass the Then action settings.



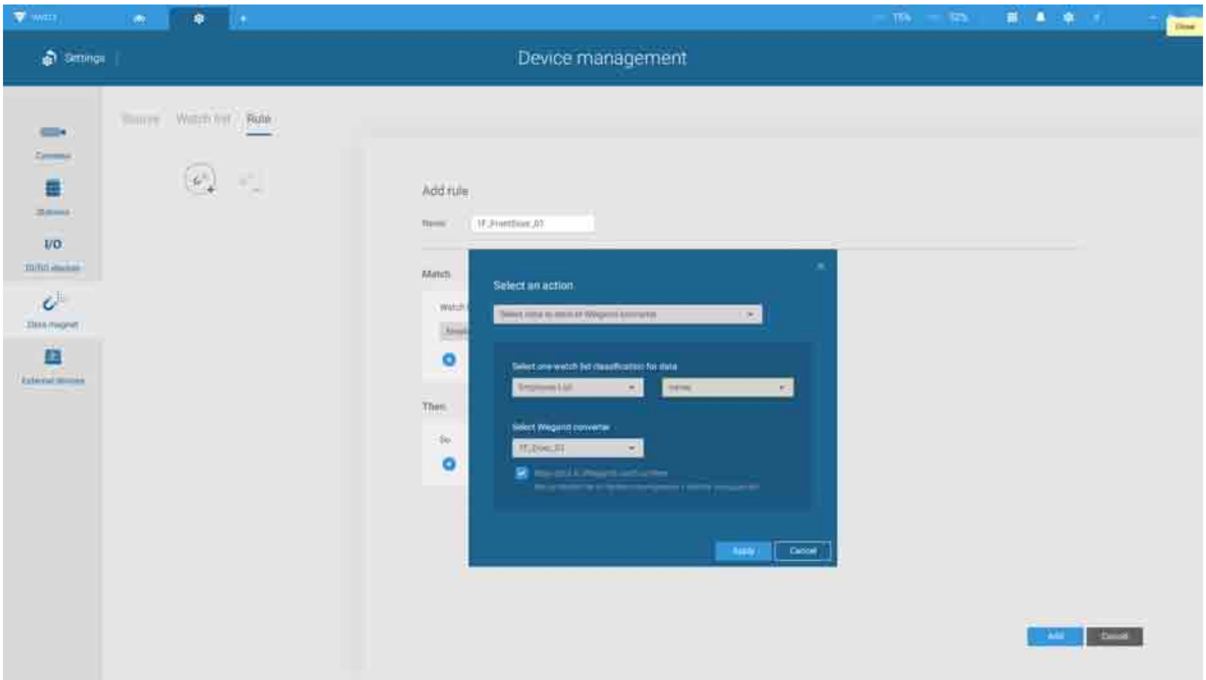
How to configure "Select data to send to Wiegand converter?"

VAST has incorporated the support for Wiegand converter AO-20W (https://www.vivotek.com/AO-20W)

The Wiegand converter can transfer the ID Badge card number through the Wiegand protocol to an access control system. The access control system then decides whether to open a gate or not. The VAST station sends an employee's card number to the Wiegand converter, the Wiegand converter then delivers it to an access control system.

To Select data to send to Wiegand converter, first select a watch list classification, and then select a Wiegand converter.

For example, a watch list's employee name=Chris and ID=90223 is verified, you can send the ID card umber to the Wiegand converter. If a watch list's data is not the card number, but the data contains name=Chris, employee ID=90223, you can select "Map data to Wiegand card number." Via the Identity management process, the identity data (such as name) is transferred into a corresponding ID Badge Wiegand card number, and then is sent to a Wiegand converter.



Name: 1F_FrontDoor_01

Select an action

Select data to send to Wiegand converter

Select one watch list classification for data

Employee List

name

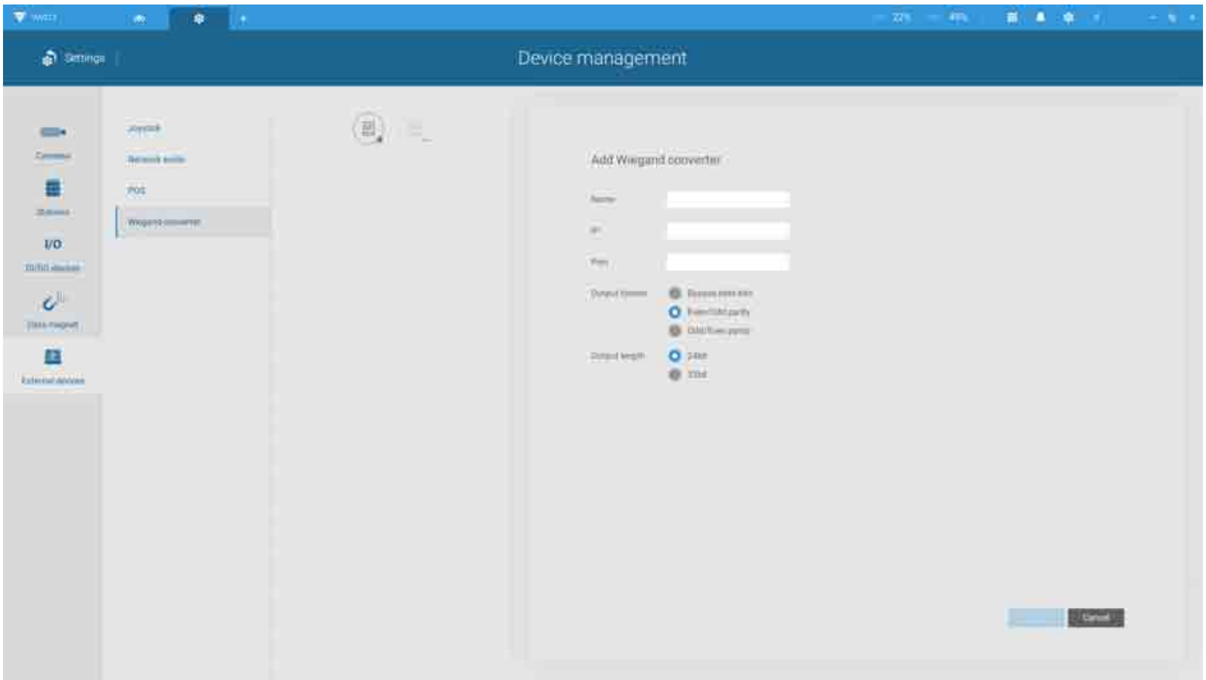
Select Wiegand converter

1F_Door_01

☑ Map data to Wiegand card number

How to add a Wiegand converter to VAST?"

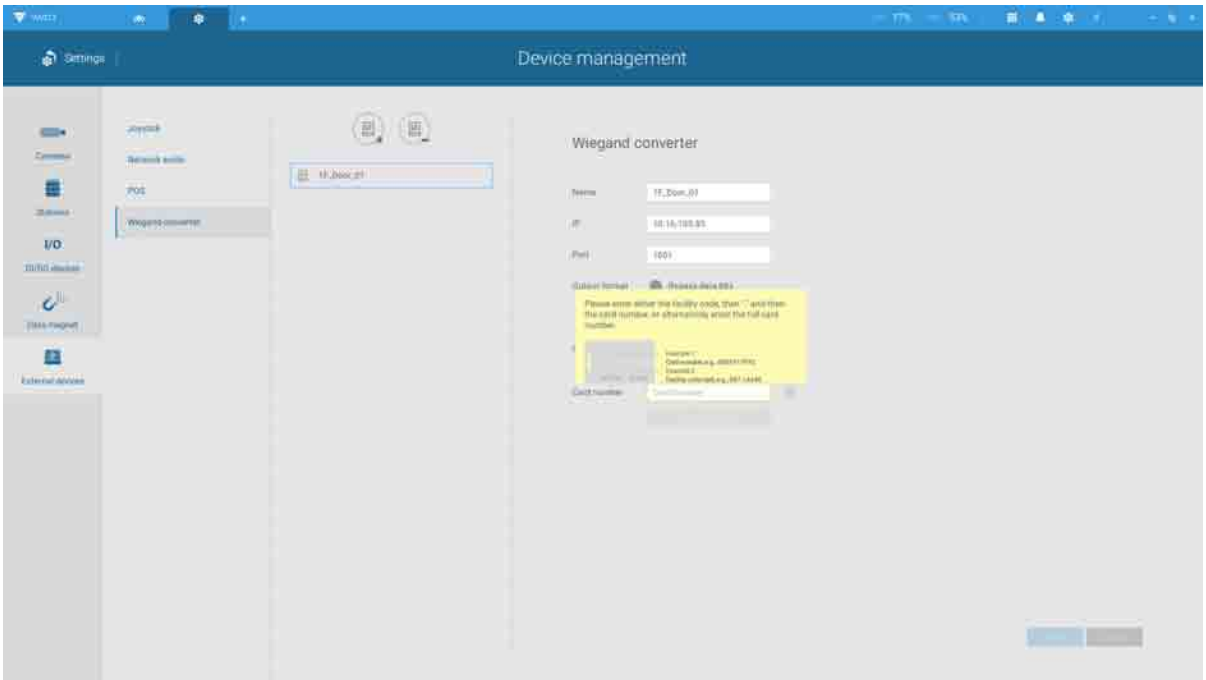
In Settings > External devices > Wiegand Converter, click the add Wiegand converter button. Enter the converter's IP, Port, Output format, and Output length. You can acquire the converter's data via a web console to it.



Add Wiegand converter

Name
IP
Port
Output format
Output length
● 24bit
○ 32bit

When adding is completed, enter a card number in the Card number field to test if the converter can successfully receive a card number.



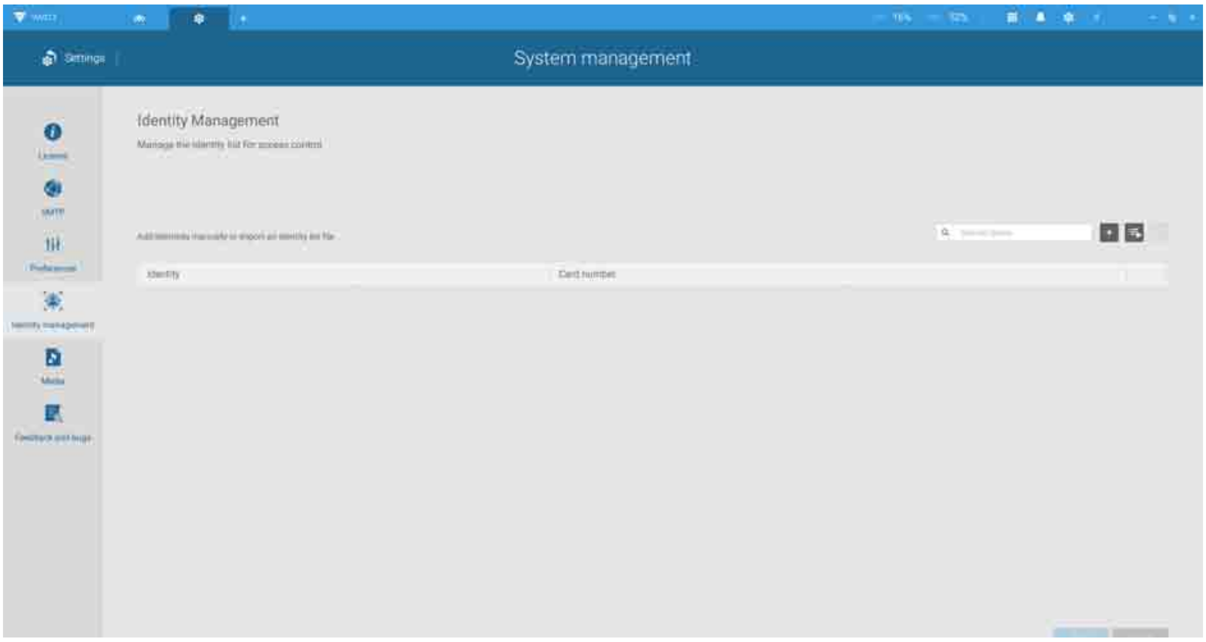
Wiegand converter

Name 1F_Door_01
IP 10.15.100.85
Port 1001
Output format
Card number

How to configure Identity management?"

In Settings > System > Identity Management, click the add an item button and enter the identity and card number.

Identity is the information such as name or employee ID or car license plate. The Card number is the ID Badge's Wiegand card number.

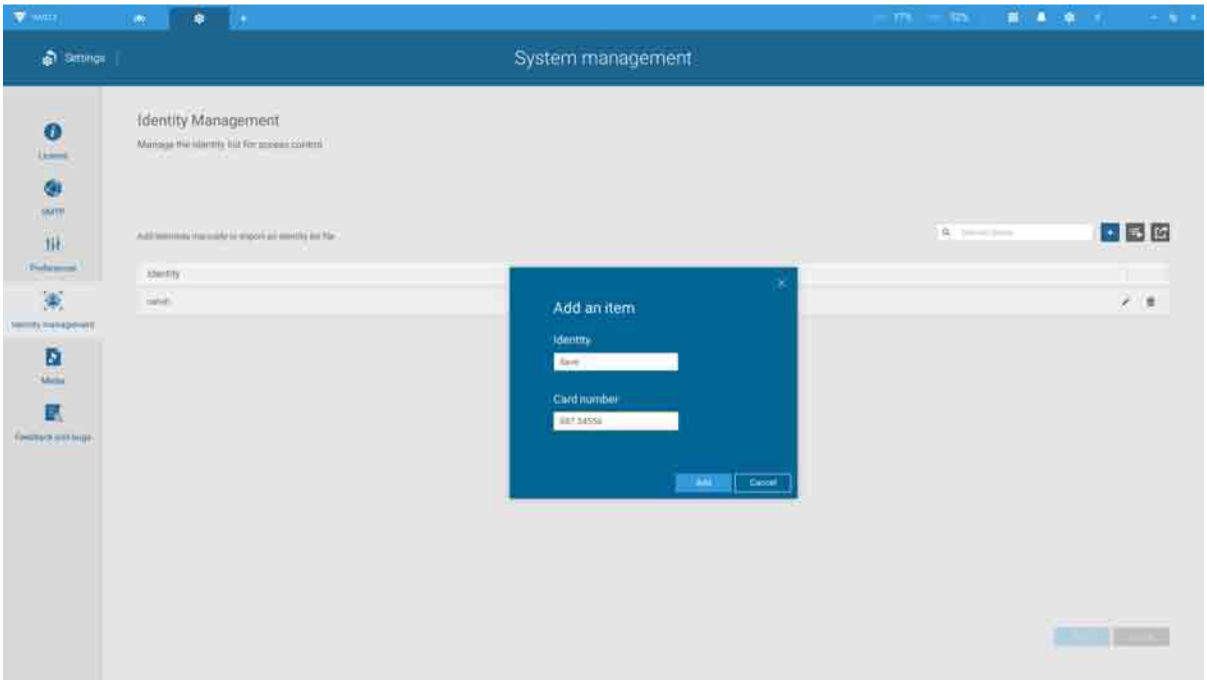


Identity Management

Manage the identity list for access control

Add identities manually or import an identity list file

Identity	Card number



Identity Management

Manage the identity list for access control

Add identities manually or import an identity list file

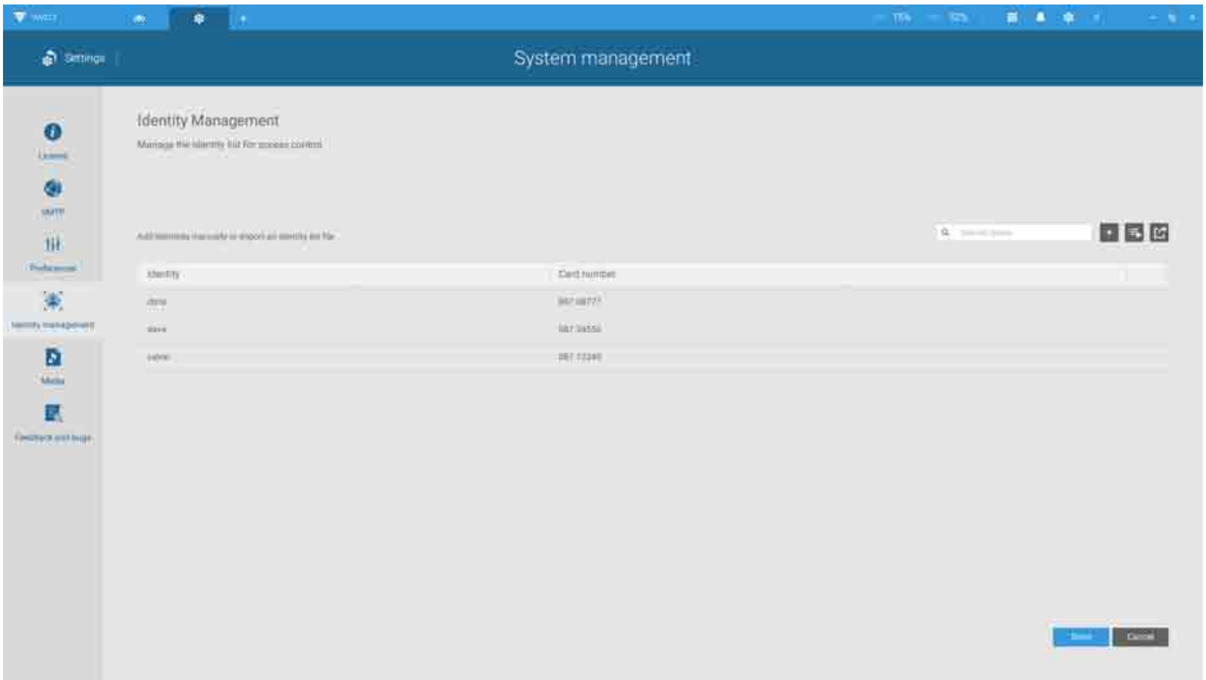
Identity	Card number

Add an item

Identity: Save

Card number: 887 34556

An identity table should look like this.



Identity Management

Manage the identity list for access control

Add identities manually or import an identity list file

Identity	Card number
chris	987 08777
dave	987 34556
calvin	987 12345