VSS

VAST Security Station

VAST Security Station User Manual

Revision Number: v1.4 Software Version: v1.2

VIVOTEK

A Delta Group Company

Table of Contents

Revision History

Rev. 1.0:

* Initial release.

Rev. 1.1:

* Release for software version 1.1.

Rev. 1.2:

* Update content for correction.

Rev. 1.3:

* Release for software version 1.2.

Rev. 1.4:

* Update content for function improvements

Introducing VSS

VIVOTEK VSS (VAST Security Station) is a professional video / central management software designed to manage all VIVOTEK IP surveillance products with intuitive functions and numerous features. It supports hundreds of cameras and stations in a hierarchical structure system for monitoring, recording, playback, and event trigger management with ease of use and efficient control.

VSS 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 solutions. VSS performs remote management with a full range of the server & client structure and constitutes a robust system for various applications, such as stores, banking, and public space.

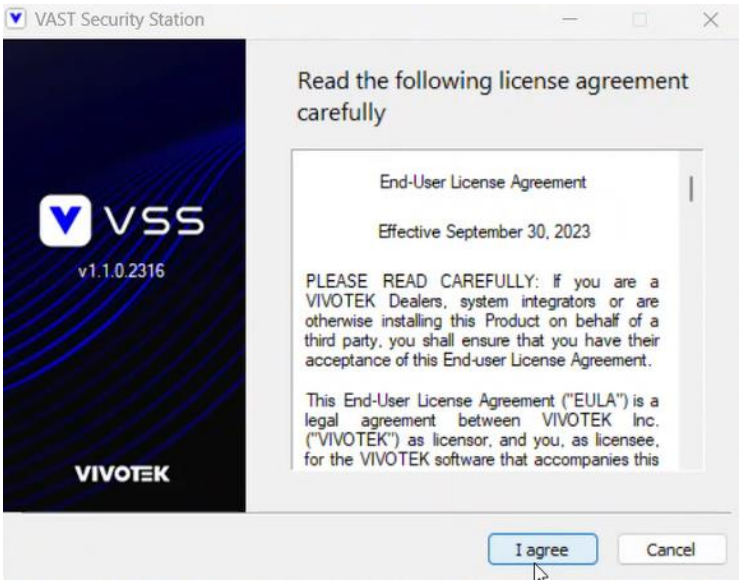
Key Features

- Deep Search with attributes, scenes, and Re-search functions
- 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 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.
- User-defined role for group authorities
- Recording encryption
- Managed PoE Switch integration

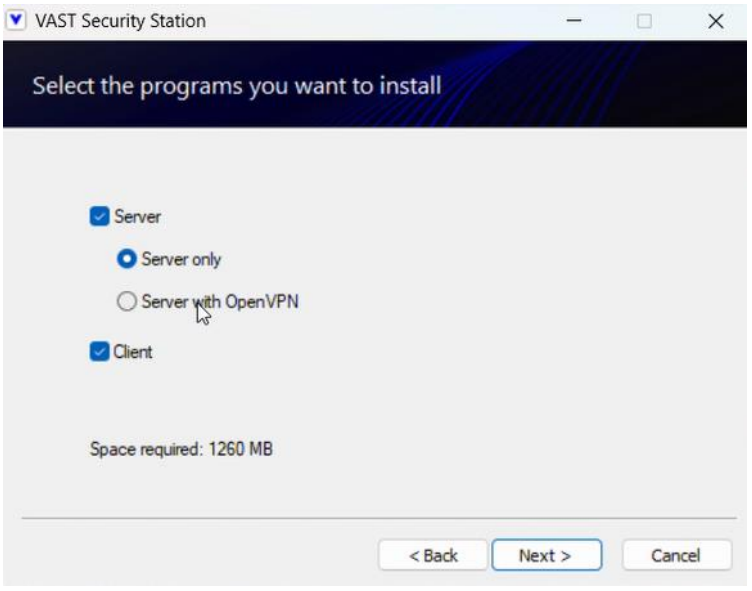
- License plate recognition solution and data magnet
- Cybersecurity Management Solution
- Smart VCA: AI Powered Video Analytics
- System Overview dashboard
- Multi-sensor display modes
- Evidence Lock: Automatically Bookmark Related Recordings When Alarm Triggered.
- Evidence Export: Manually Export Video Recordings or Alarm Clips.
- Matrix for Video Wall Solution
- Automatic Problem Feedback Mechanism
- Multiple Fisheye Dewarp Modes

Installing VSS

1. Run the vss_setup_version_(x64).exe on your computer.
2. Read the license agreement carefully and click “I agree” to initiate the installation process.

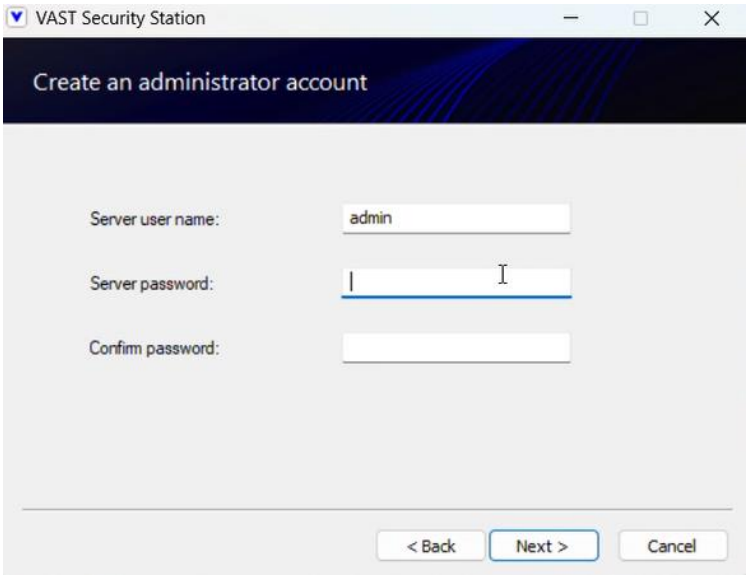


3. Select the programs you want to install, then click “Next” to continue. Refer to the “Installation Option” section for more information on the “Server with OpenVPN” option.

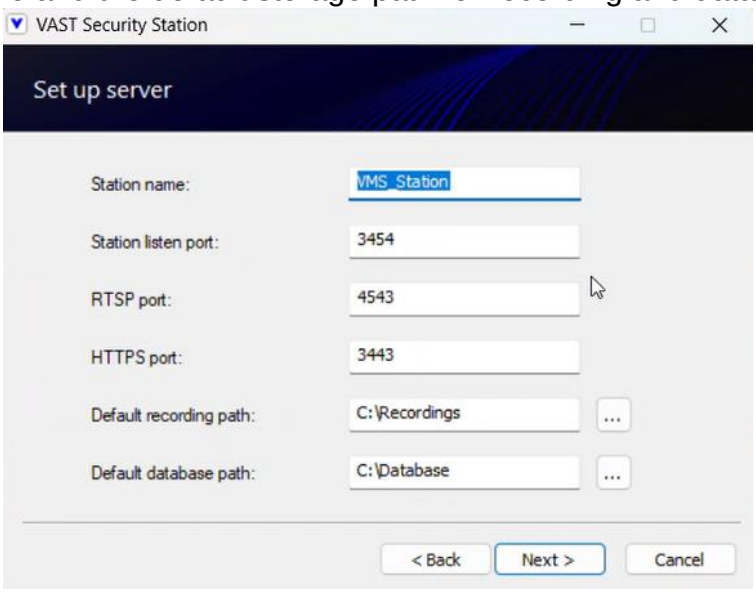


4. Select the server type you want to install, then click “Next” to continue. Your first installation of a standard server includes a 60-day trial of the VSS Pro edition, and you will need to purchase the official software licenses for continued use after the trial expires.

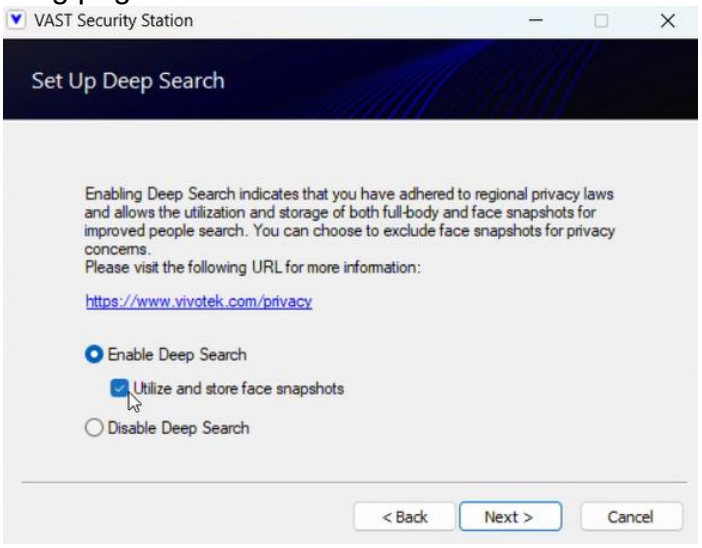
5. Create an administrator account.



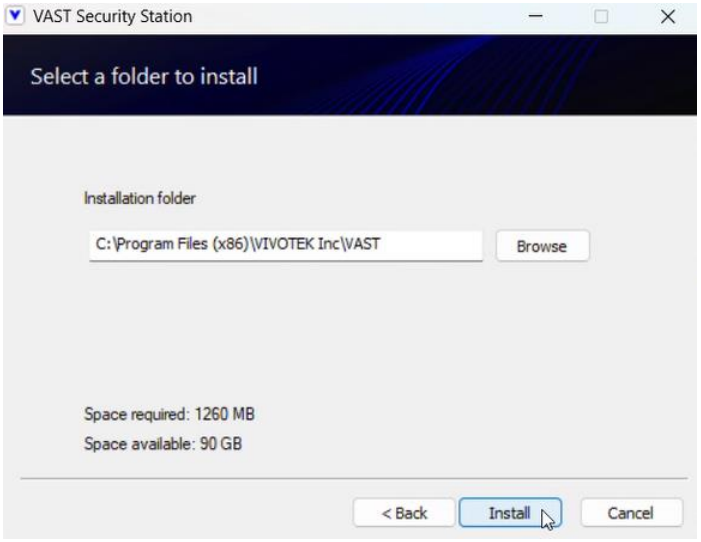
6. Set up the name and the default storage path for recording and database.



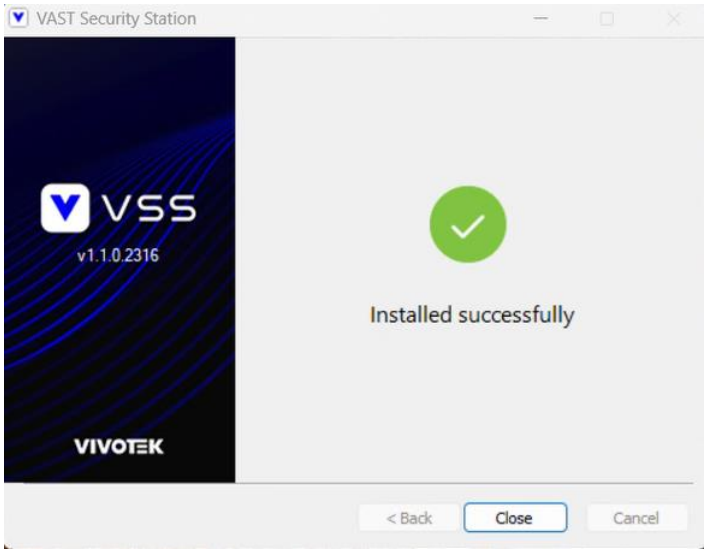
7. Choose whether to enable VSS to utilize and store person attributes and full-body/face images for improved people search. If you prefer to exclude face snapshots, uncheck the “Utilize and store face snapshots” checkbox. This setting can also be modified on the VSS client setting page after installation.



8. Specify a location to install the software, then click “Install”.



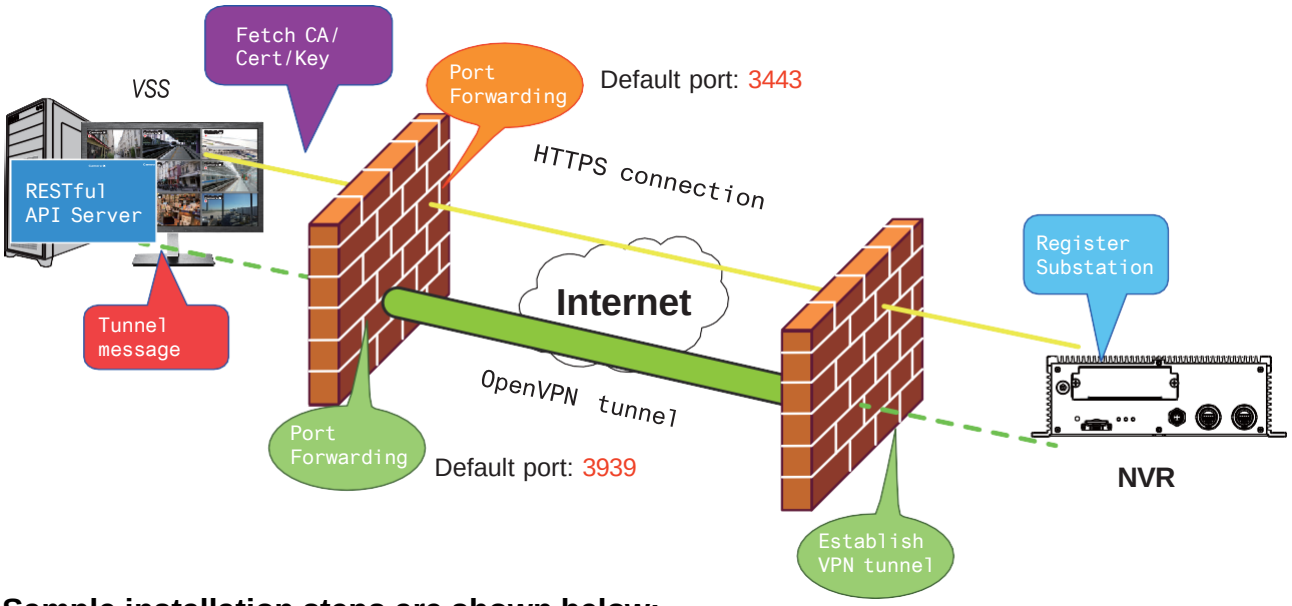
9. Wait for the installation process to complete, then click “Close” to exit the installation process.



Installation Option

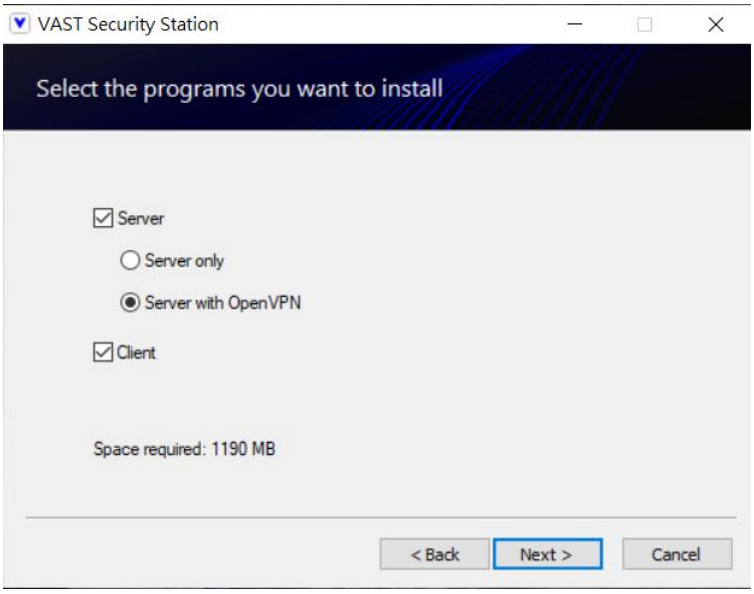
NAT-traversal with OpenVPN

A remote connection between a VSS server and an NVR with 3G/4G/LTE network can be made through an OpenVPN tunnel. The figure below shows the methodology comprising HMAC authentication and TLS encryption over an encrypted UDP connection.



Sample installation steps are shown below:

Step 1: Install VSS by selecting the Server with OpenVPN option.



Step 2: Enable the public IP of the VSS Server.

For the NVR to establish an OpenVPN connection with the VSS Server, the user must activate the public IP of that server. (Note that the specific steps depend on the user's network environment and relevant IT policies.)

After activating the Public IP, ensure the accessibility of the HTTPS port and OpenVPN port. (Note that the VSS OpenVPN port by default is 3939, so the user must set up port forwarding with UDP.)

If the default HTTPS port (3443) is unavailable, the user must modify the corresponding port number under VSS Settings > Device > Stations. If the default port for OpenVPN (3939) is not available, the user needs to modify the configuration file of OpenVPN (located in C:\Program Files (x86)\VIVOTEK Inc\VAST\Server\OpenVPN\config\server\server.ovpn).

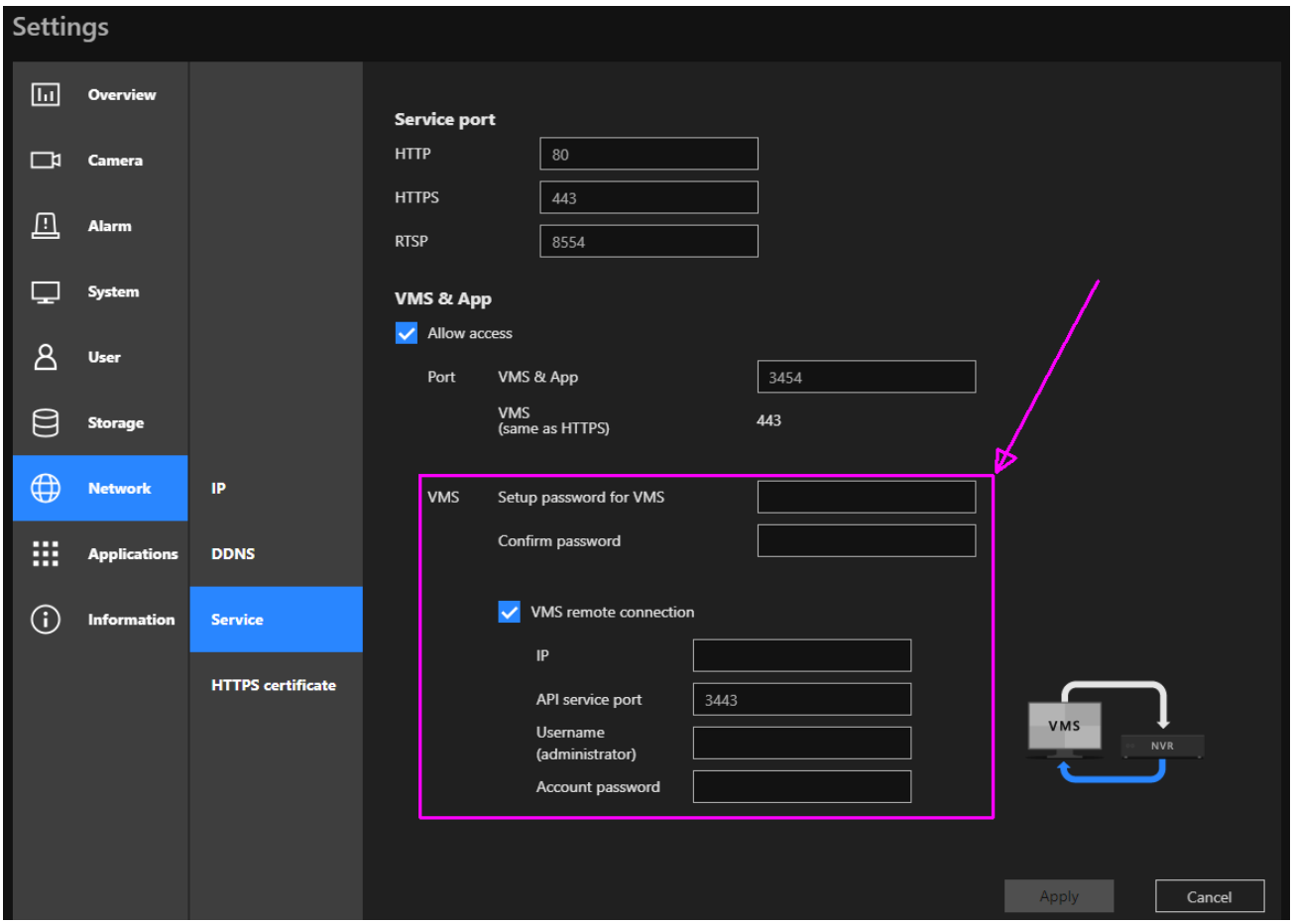
You can directly edit the port number in this text file (file content is shown below):

```
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 10 120
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
compress lzo
```

Step 3: Configure the NVR OpenVPN connection.

Once you have obtained the VSS Server public IP, configure the NVR settings under Network > Service > CMS. Then, enter the VSS server public IP/credentials/API service port (HTTPS). (Note that if the HTTPS port on the VSS end is not 3443, you must modify the corresponding port number.)

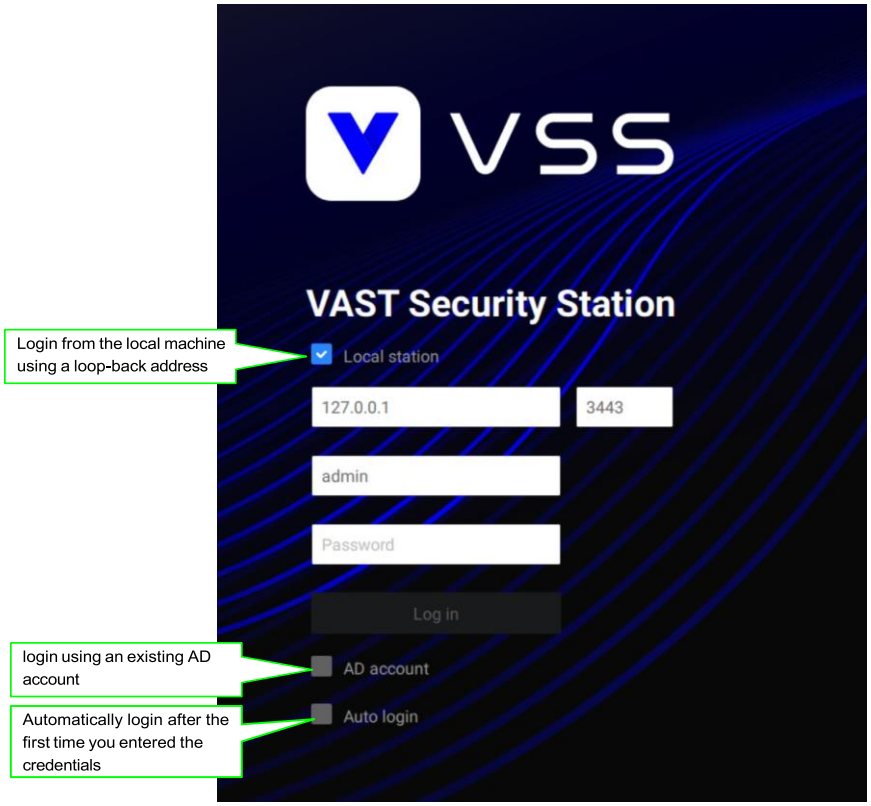
After configuring the settings for VSS and NVR, the OpenVPN connection will be established. Once the connection is established, this NVR will be automatically added to the VSS server. (Note that the NVR and VSS server should have a similar time setting when exchanging certificate information. Otherwise, the mutual handshake authentication process may fail.)



Log In

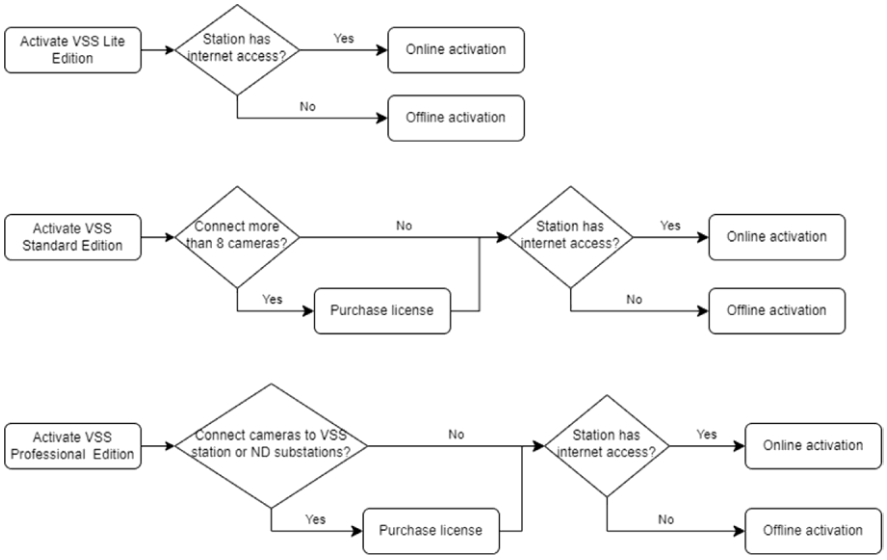
To log in:

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 account to log in. Please refer to Settings > User Management > Add a New User Account - Windows AD Account for 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 VSS software.



VSS Software License

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



After VSS is installed, a 60-day trial version will be started automatically.

Users must select one VSS edition and activate the license online or offline before the trial expires. Otherwise, the camera live view, playback, and recording services will stop after a 60-day trial. Users can use the edition selector on the VSS website to select the suitable VSS edition and use the license calculator on the download page to calculate the required license.

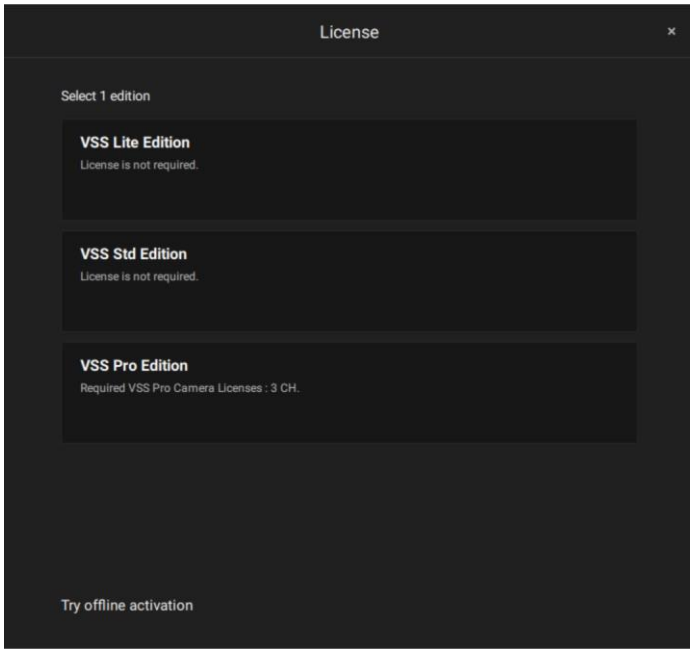
Online activation

If the VSS station has internet access, activate the license using the online activation method. The license request file of the VSS station (.req file) will be sent to the licensing server automatically via the internet. The licensed file (.lic file) will be received from the licensing server if the activation process is successful.

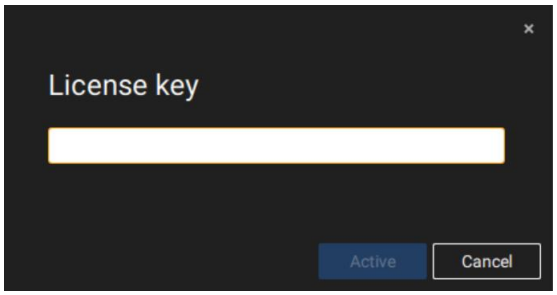
Online activation is recommended over offline activation. However, if online activation fails or internet access is unavailable, see Offline Activation in the next section below.
Steps:

The edition menu will show if you must purchase licenses to activate each edition based on your current VSS deployment.

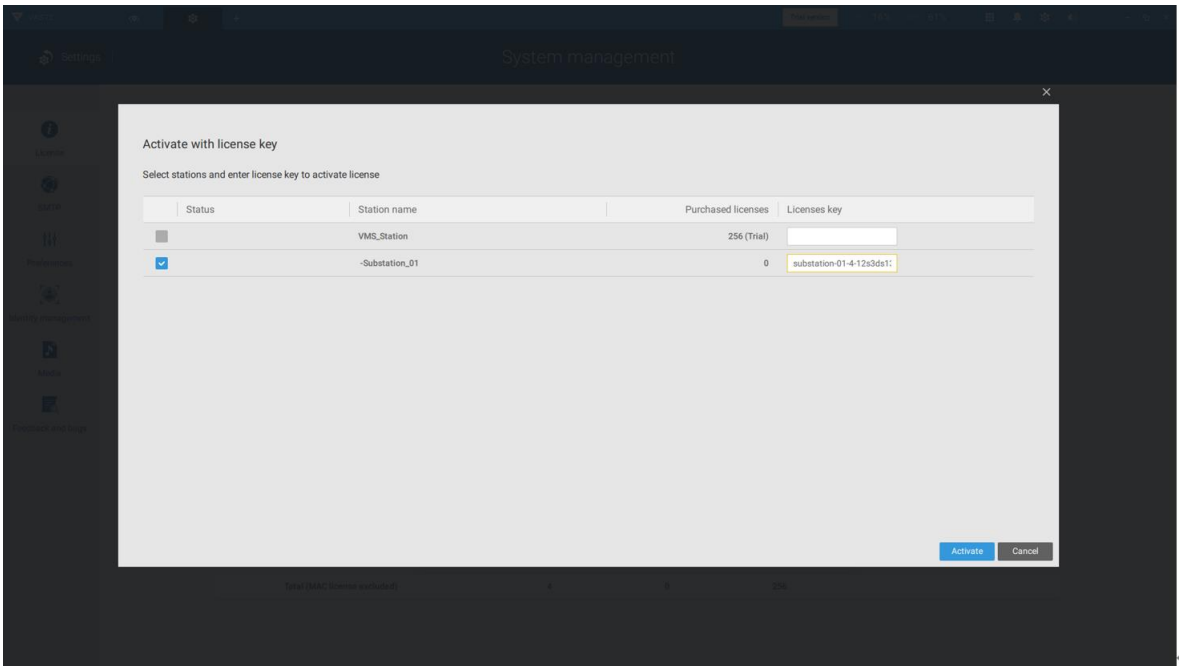
If the purchased license is not required, click on the edition, and the activation process with the licensing server will begin.



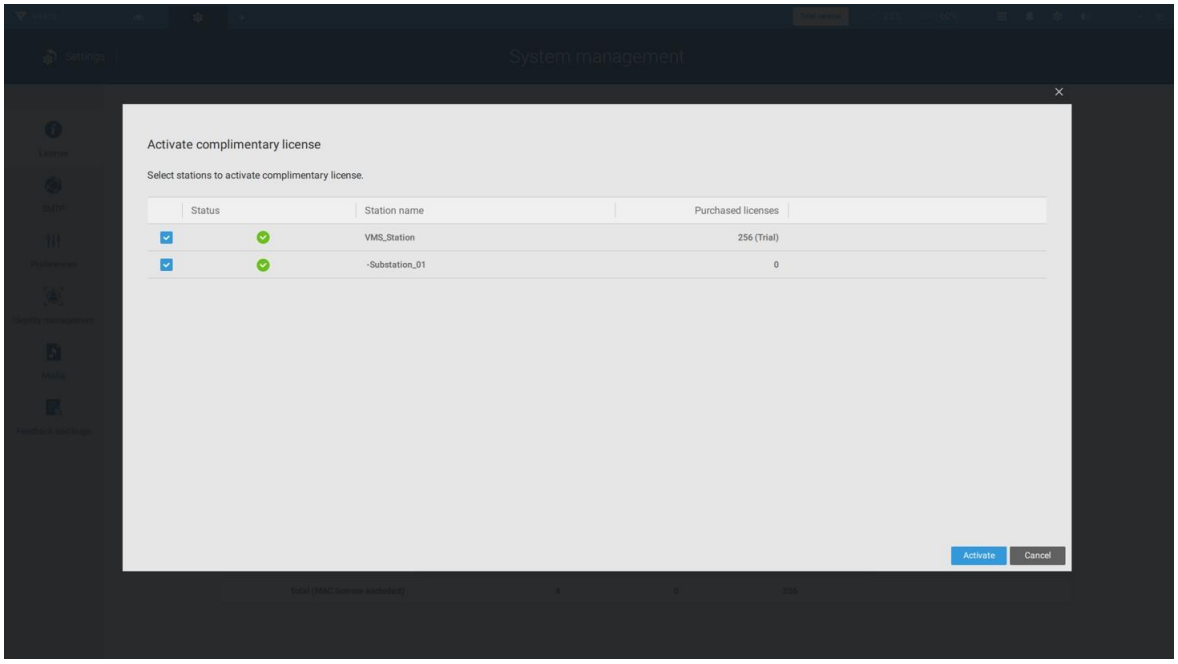
If the purchased license is required, a license key window will pop up after you select the edition. Type in the license key you purchased and acquired from your distributor or VIVOTEK local sales and click Activate, then the activation process with the licensing server will begin.



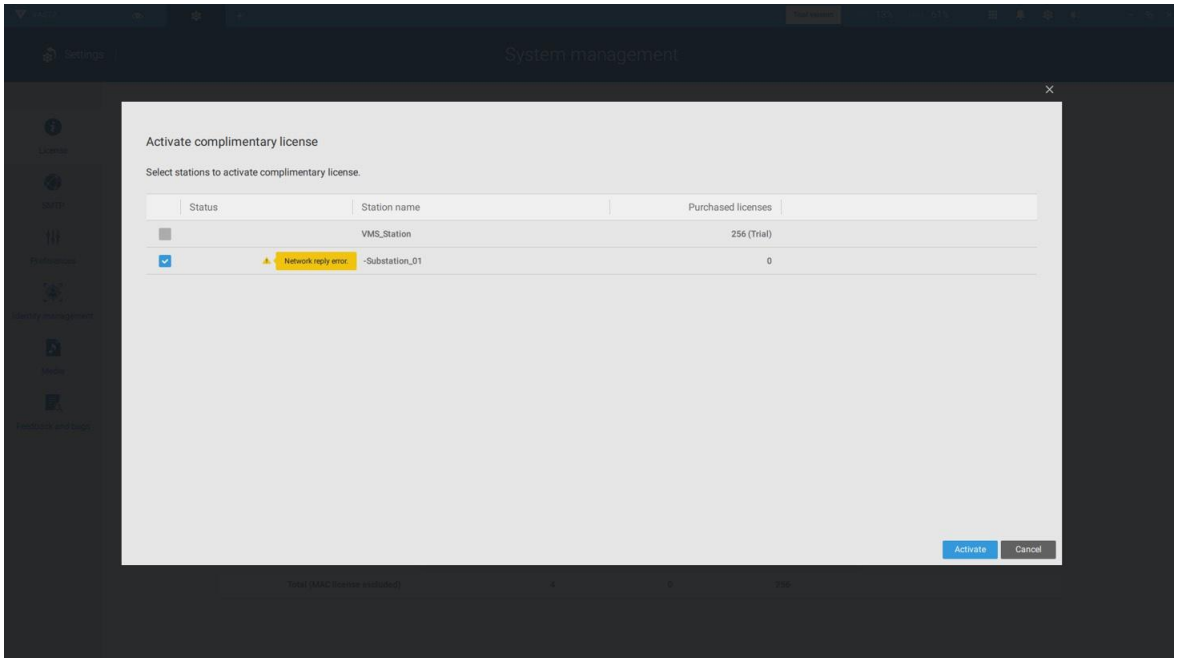
If you select **Activate with license key**, select the station where the license key will apply to. Enter the license key.



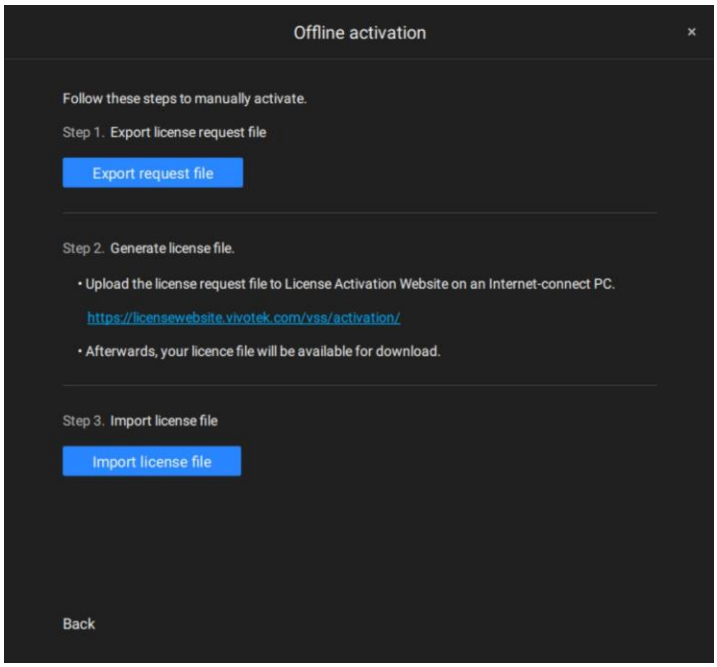
When successfully activated, the associated check circles will turn green. Click the Close button on the upper right of the screen.



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

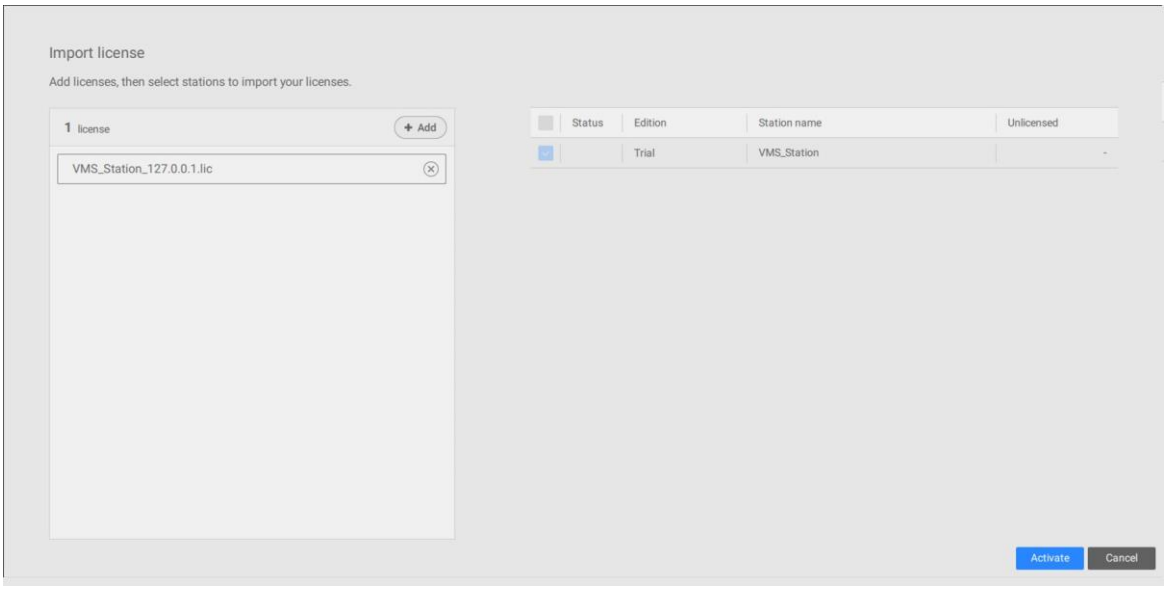


If your VSS station has no Internet connection, Click Try offline activation.

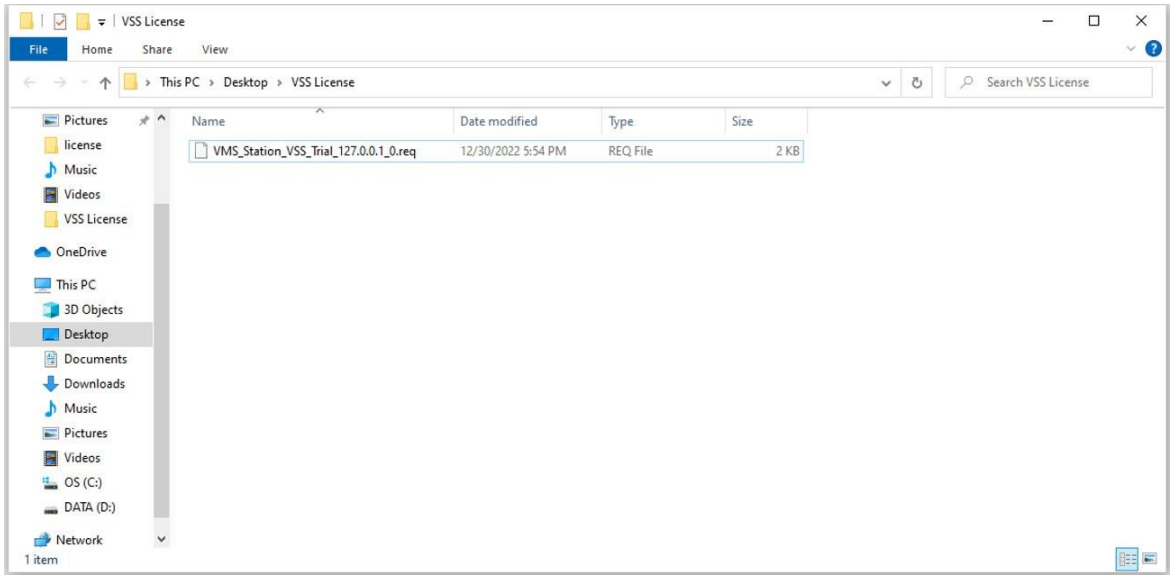


According to the instructions on the screen,

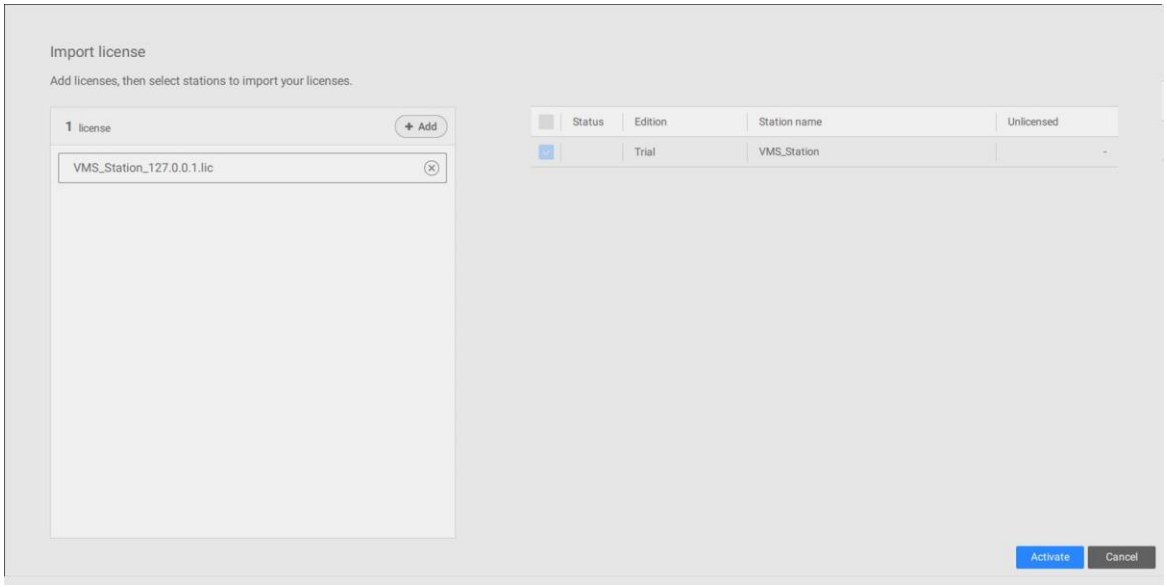
1. Export license request file.
2. Select the station to export the license request, click Export, and select the destination of the request file.



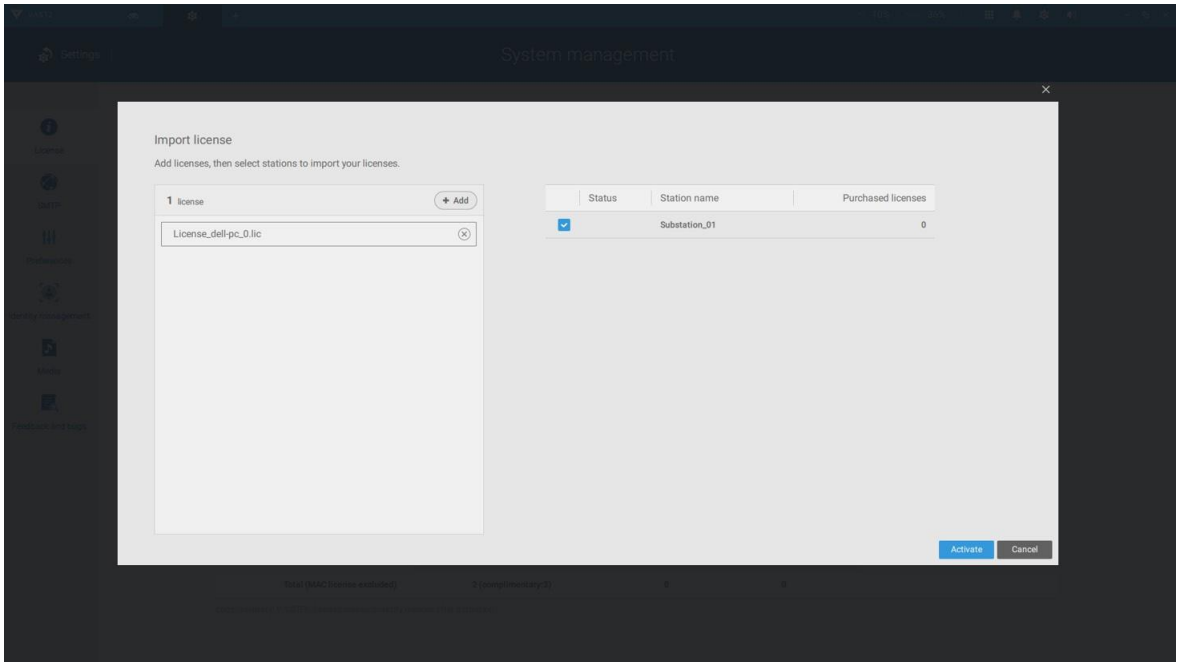
The REQ file looks like the following.



3. Find a computer to upload the license request file (.req) to VIVOTEK's license activation portal at https://licensewebsite.vivotek.com/vss/activation/.
4. Follow the instructions on the license activation portal to generate and download the license file (.lic). Upload or copy the file to your VSS station.
5. Return to the offline activation window on your VSS station, select Import license file, click Add to select the license file (.lic), and click Activate.



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



License Protection Mechanisms

The software license is verified by identifying the unique characteristics of the user's PC. The license file contains data on the VSS station's basic hardware configuration (Motherboard, CPU Processor, Graphics Card, RAM, and Network Card). The software license will become invalid if the user changes any three of these essential hardware components. For VSS Professional running on a Virtual Machine (VM; supporting VMware and Microsoft Hyper-V), the license is tied to the MAC addresses of the VM's network cards and the VM UUID. Any changes to these identifiers or alterations in the number of network cards within the VM will invalidate the license.

NOTES:

• Keep a copy of the license key, license request file(.req), and license file (.lic) for future reference.

• Without sufficient licenses, the camera live view, playback, and recording services will stop in 14 days.

• The VAST1 license, VAST2 license, and dongle license are incompatible and unable to be used as the VSS license.

• An identical software license applies to VIVOTEK and ONVIF cameras. You do not need to activate two different kinds of software licenses.

• If the VSS server application is removed and re-installed, the number of licensed channels remains intact.

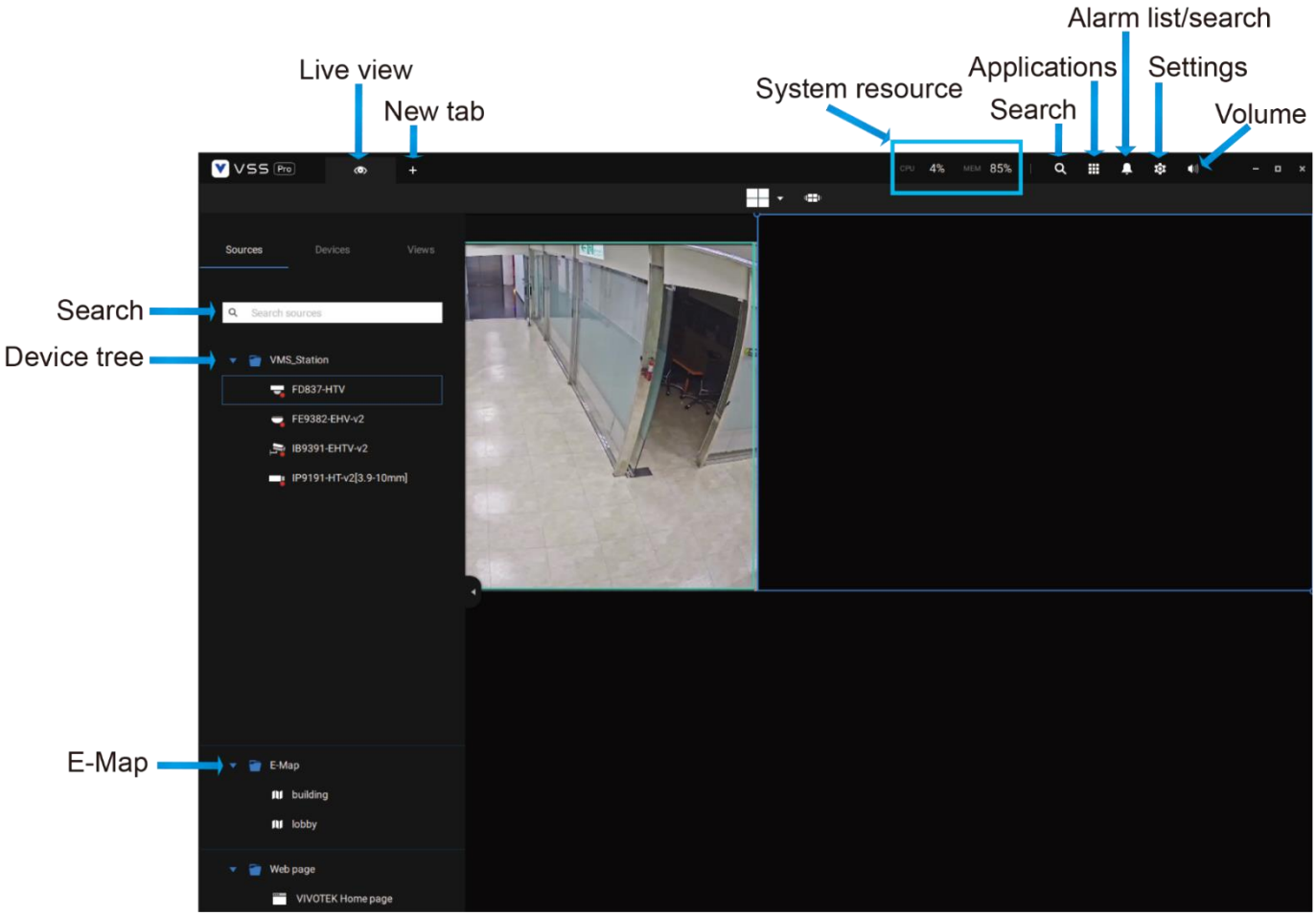
• Users can upgrade the VSS edition by activating appropriate edition licenses. Downgrading the edition via the license is not supported.

Chapter 1: Basics:

Control and Elements

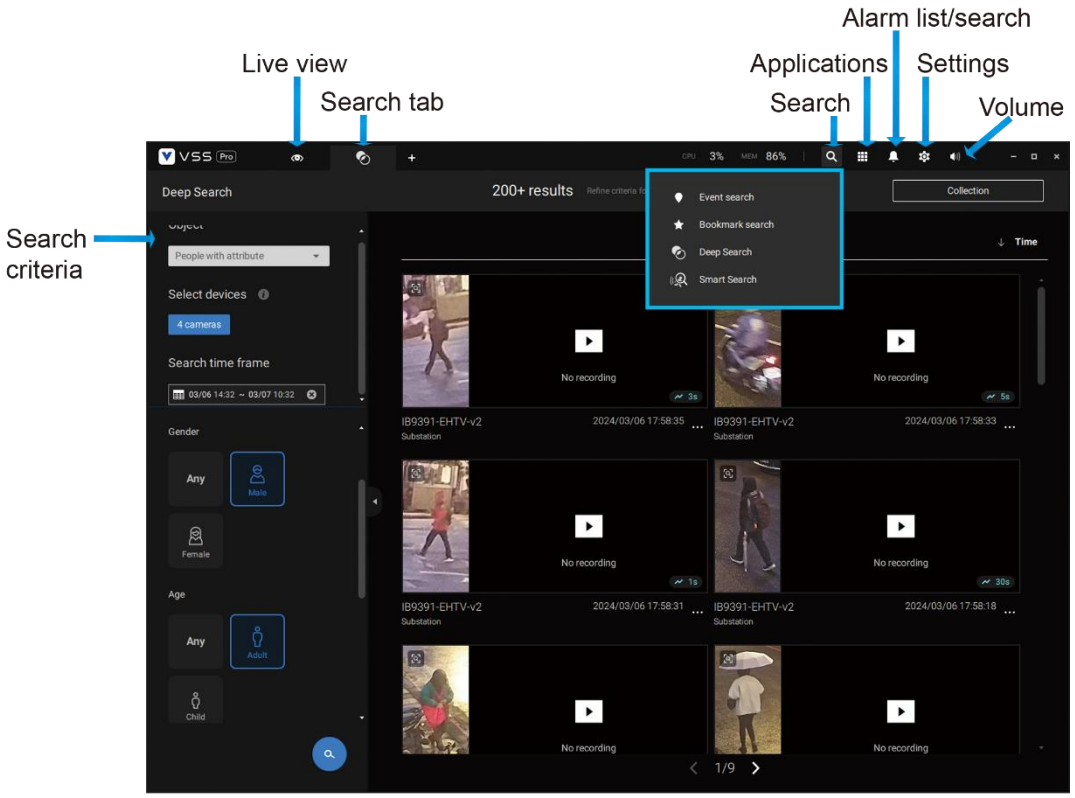
The basic screen elements of VSS live view, playback, and search panel are shown below:

Live view

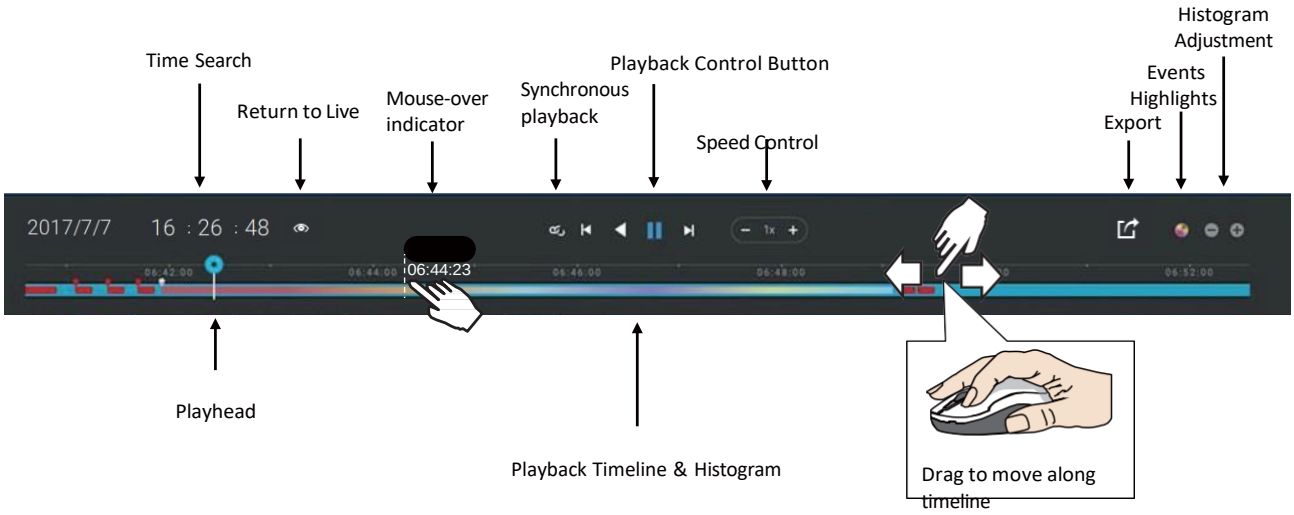


Playback is evoked when a view cell is selected, and you click the Playback button ▶ on the upper right of the view cell.

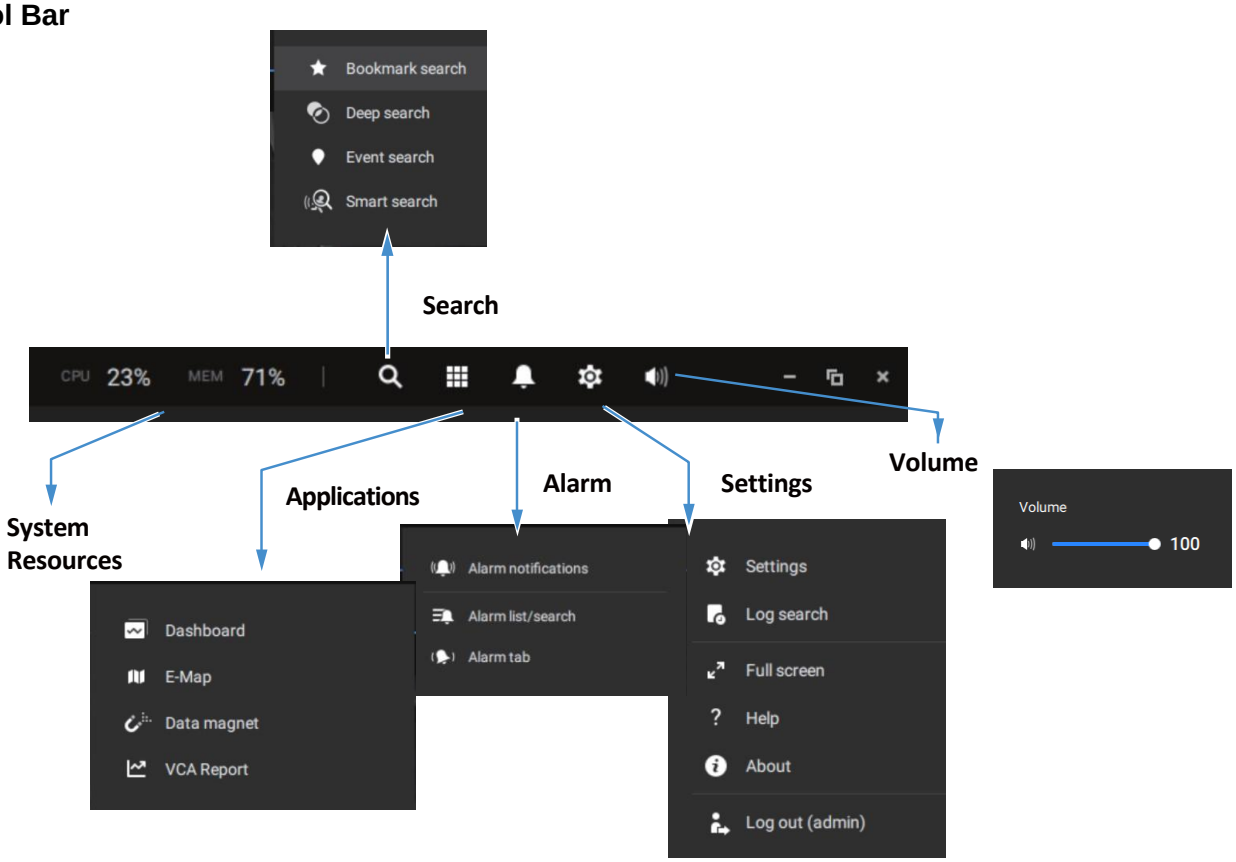
Search Panel



Playback Control

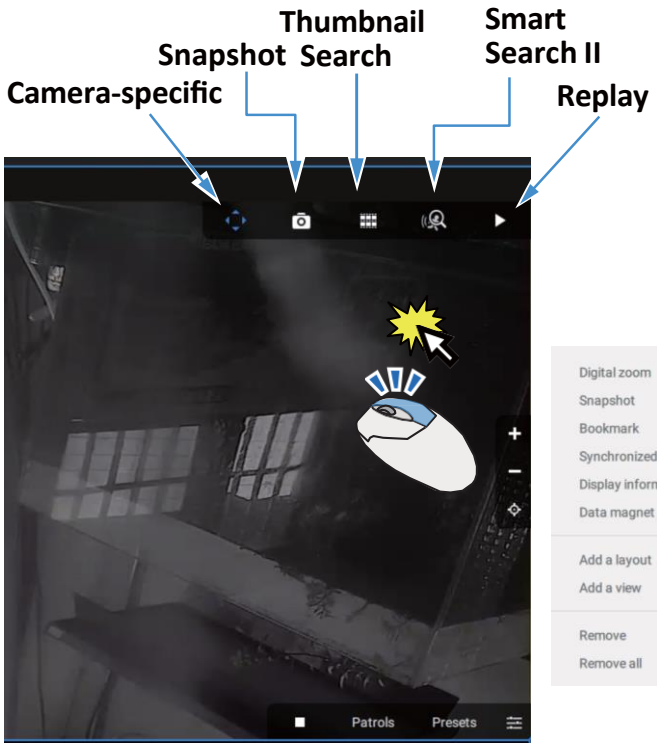


Top Tool Bar


Bookmark search
Deep search
Event search
Smart search
Search
CPU 23%
MEM 71%
System Resources
Applications
Alarm
Settings
Volume
Dashboard
E-Map
Data magnet
VCA Report
Alarm notifications
Alarm list/search
Alarm tab
Settings
Log search
Full screen
Help
About
Log out (admin)
Volume
100

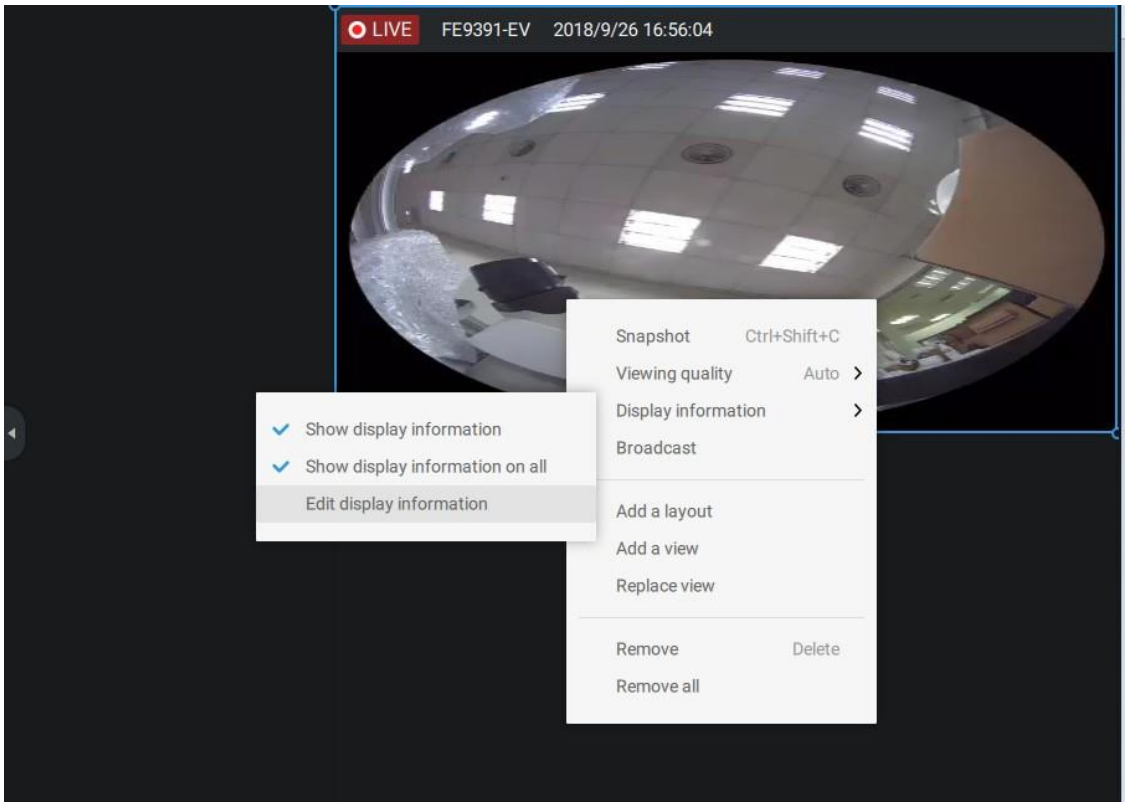
View cell control

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



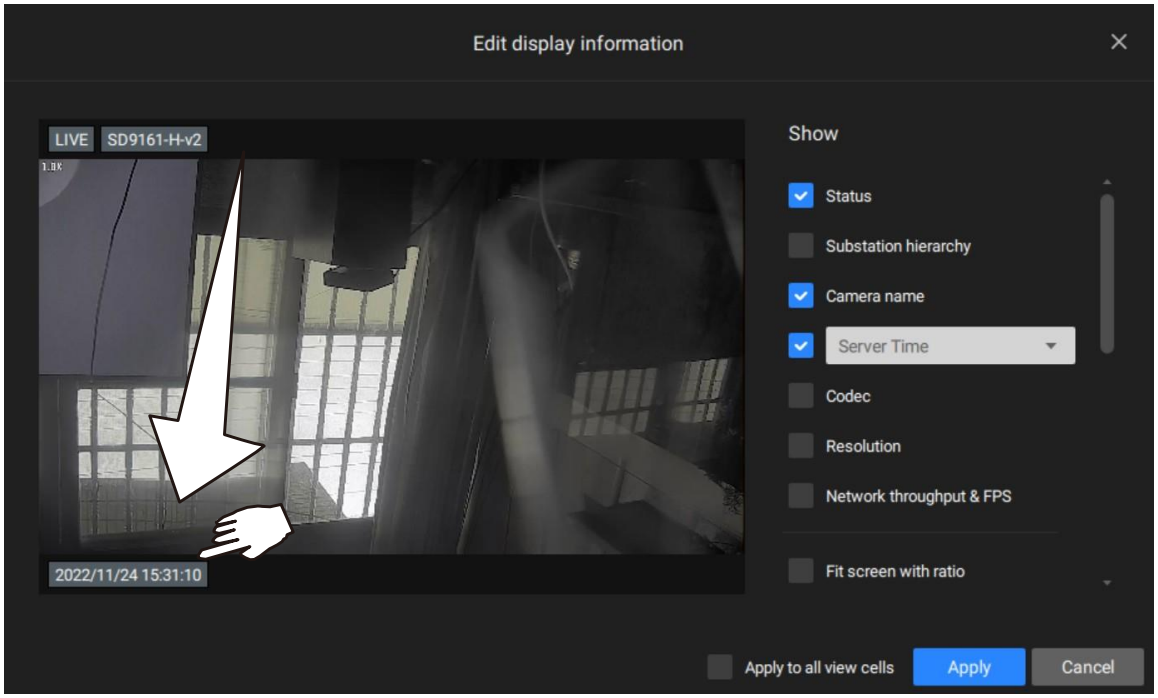
Text overlay

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.

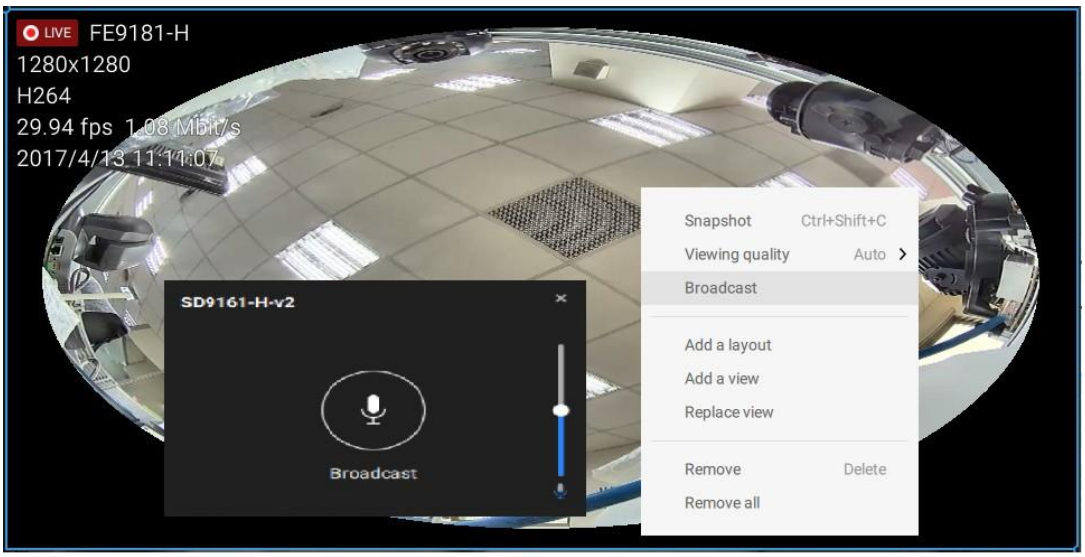
You can apply your current configuration to all view cells by selecting the **Apply to all view cells** checkbox. Note that you can also display the VCA rules and areas on the screen.



Two Way Audio

If your cameras support the Two Way Audio feature and the microphone and audio output to 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 VSS software supports 1 to 1 broadcast.



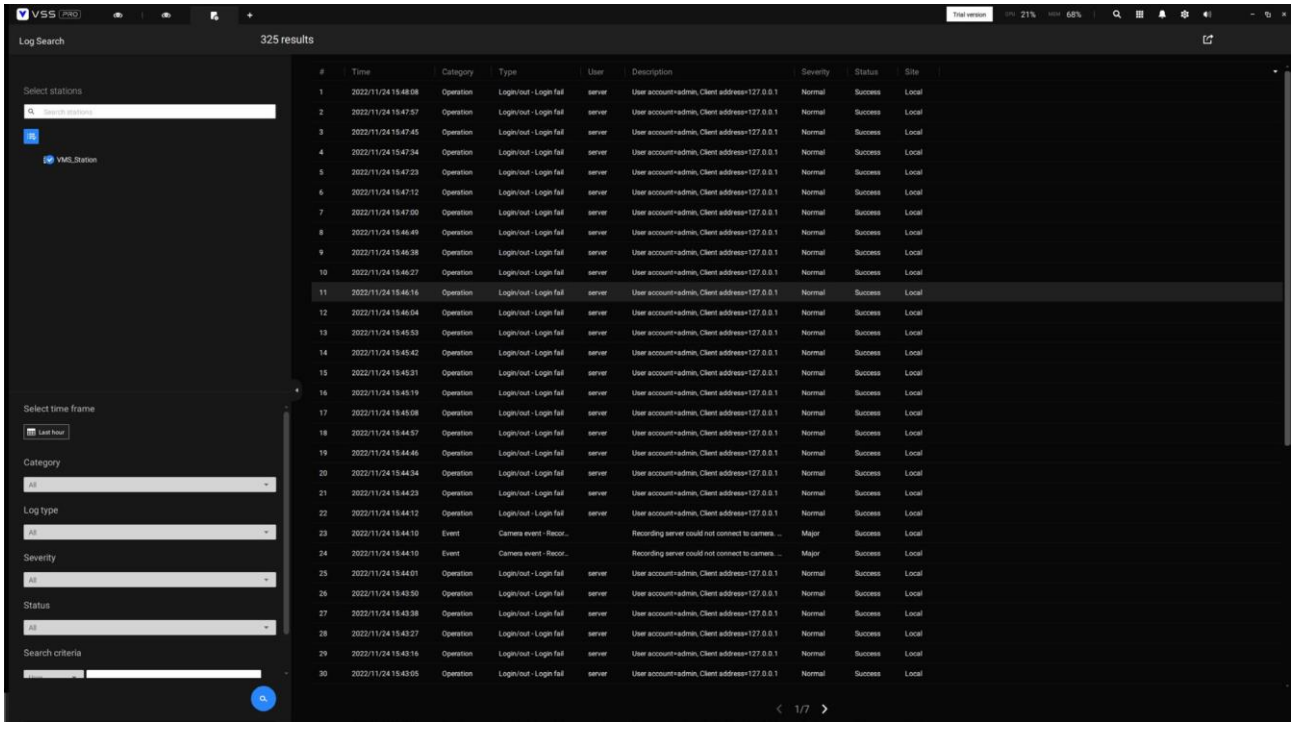
Full Screen

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

Log Search

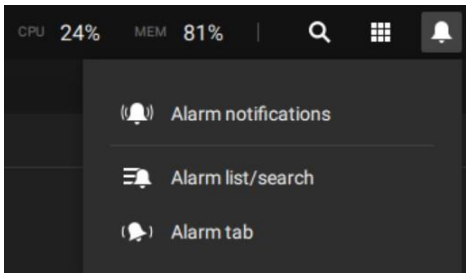
System logs can be found via the toolbar tab. All system events will be listed in the Log search panel. If you have multiple servers or substations, select a server. You can search specific events by the event types (All triggers, camera, system/station, external devices), or by the time of occurrence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

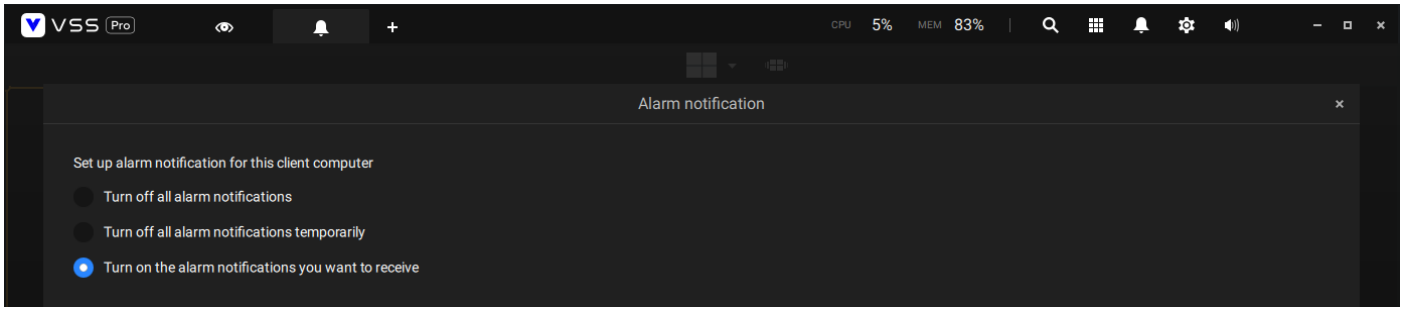
Use the Export button  to export the system log as an individual log file.



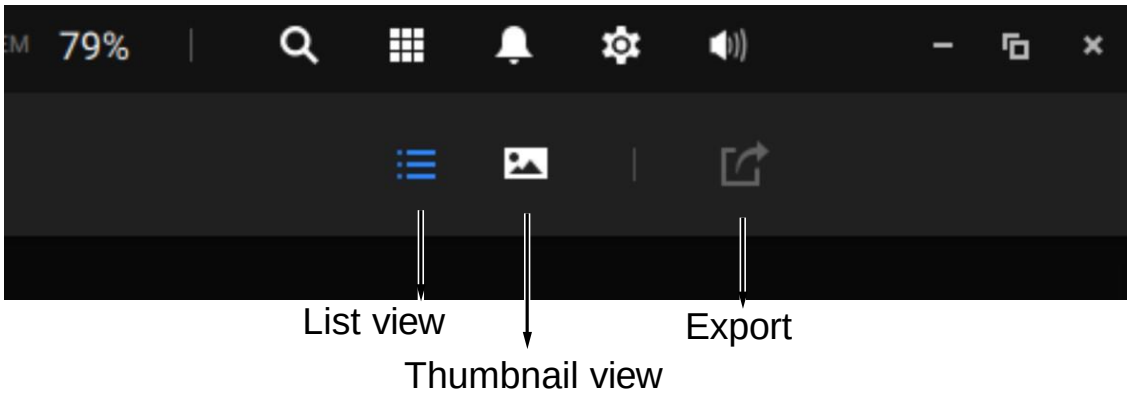
Alarm list

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

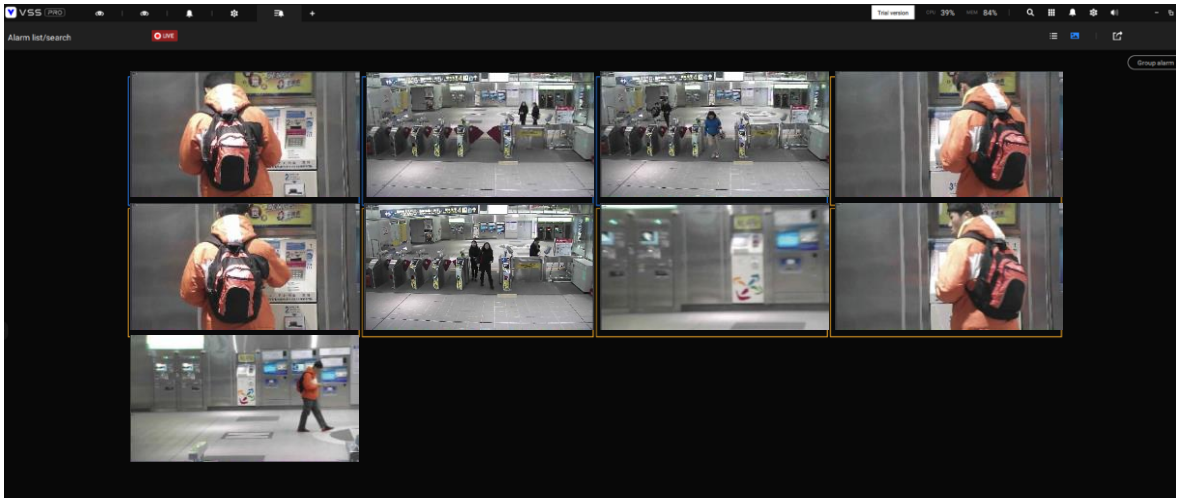




The Alarm list can be displayed in either the List view or Thumbnail view.



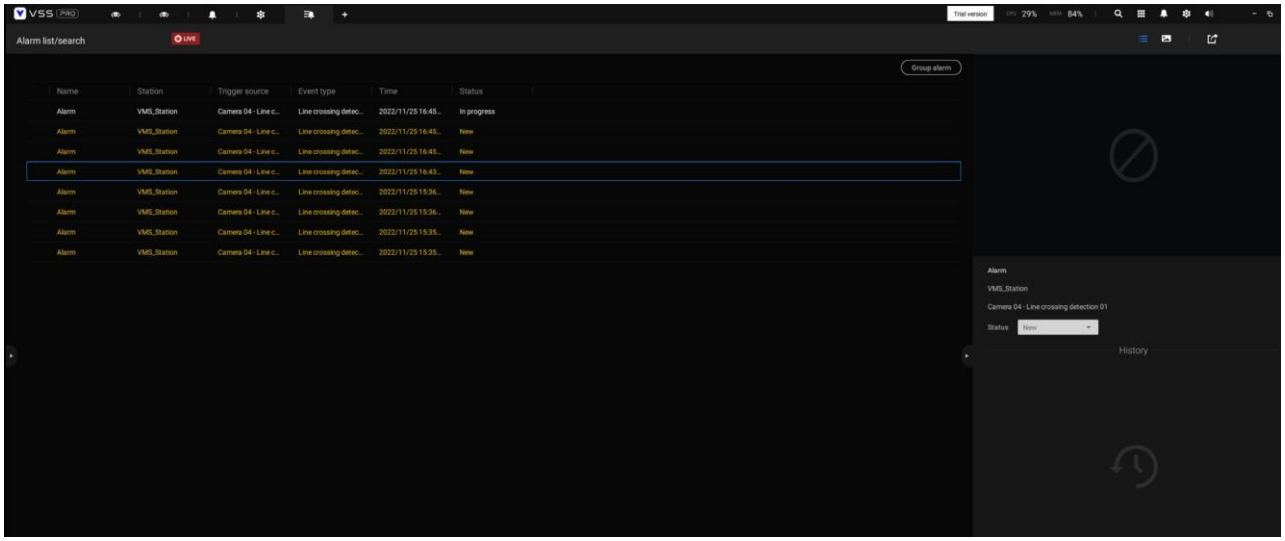
Below is an example of a Thumbnail view.



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

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

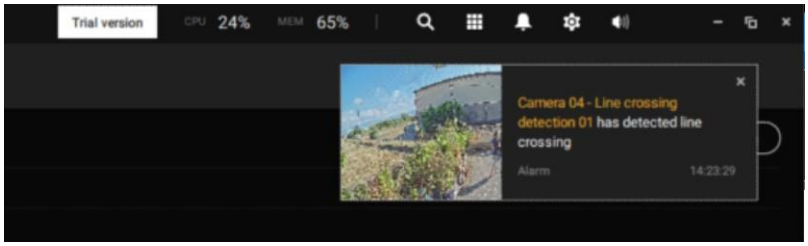
When done with designating event status, click the Acknowledgement button.



The Alarm list also supports Hot keys.

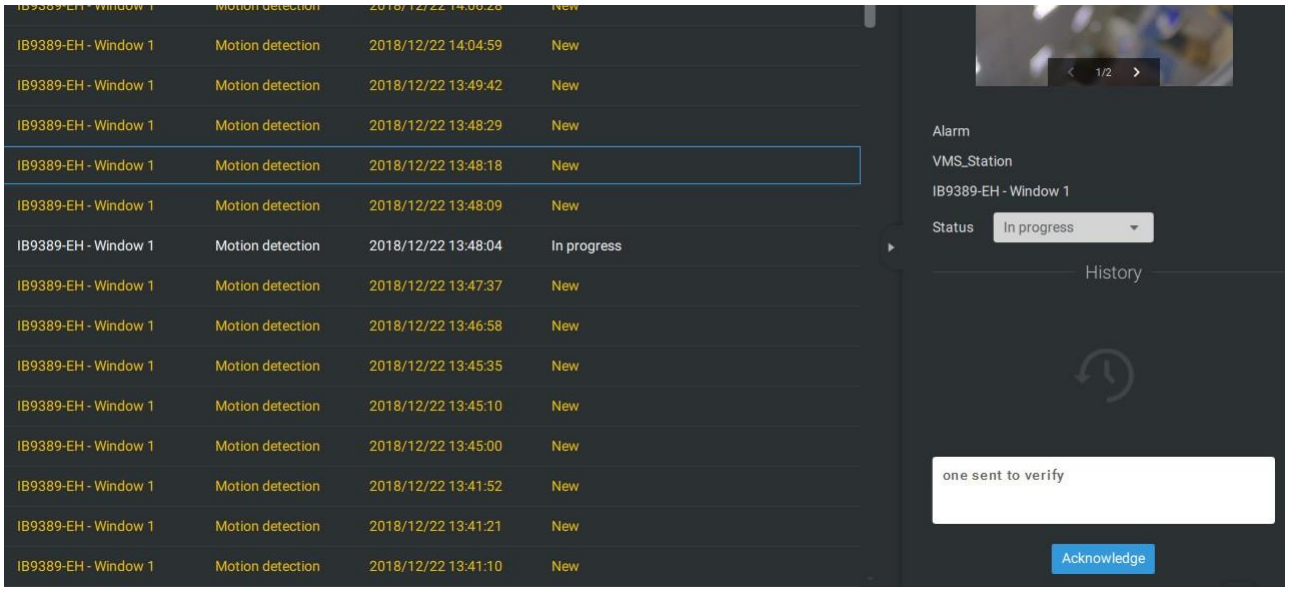
Alarm list window			
Mute the current alarm	Ctrl		m
Designate the selected alarms as false alarms	Ctrl		f
Select all alarms	Ctrl		a
Select one or multiple alarms	Ctrl		left mouse button
Select multiple alarms		Shift	left mouse button
Select different alarms			Up/Down/Left/Right

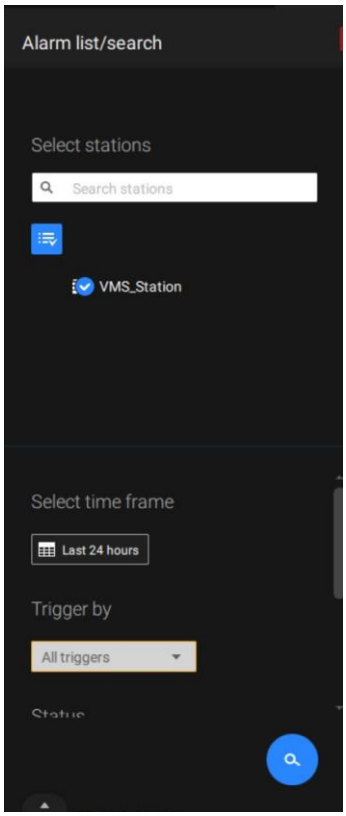
When an alarm is muted, a message will prompt asking for how long the alarm will be muted. Enter a number, and the alarm will disappear from the list temporarily.



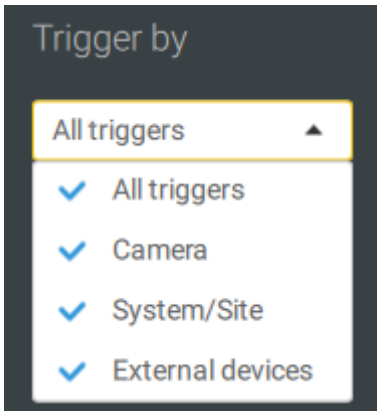
When an alarm is designated as a false alarm, it is immediately removed from the list.

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

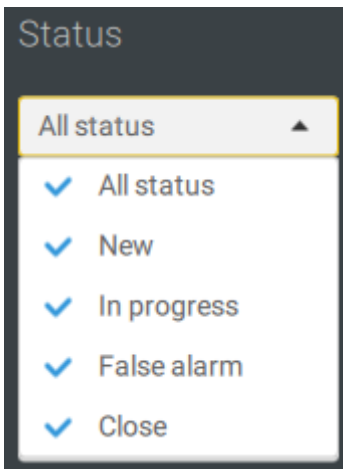




To find alarms of specific types, time of occurrences, and alarm status, click the side tab to reveal the search panel.



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



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

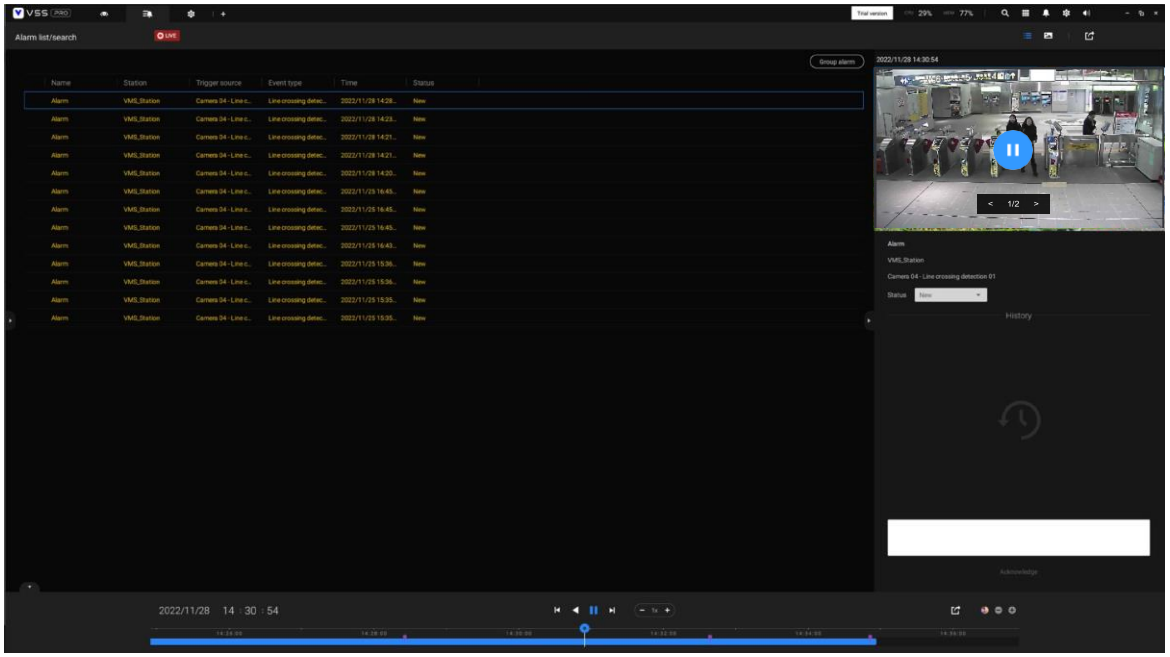
You can enter one or multiple keywords as the search criteria.

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

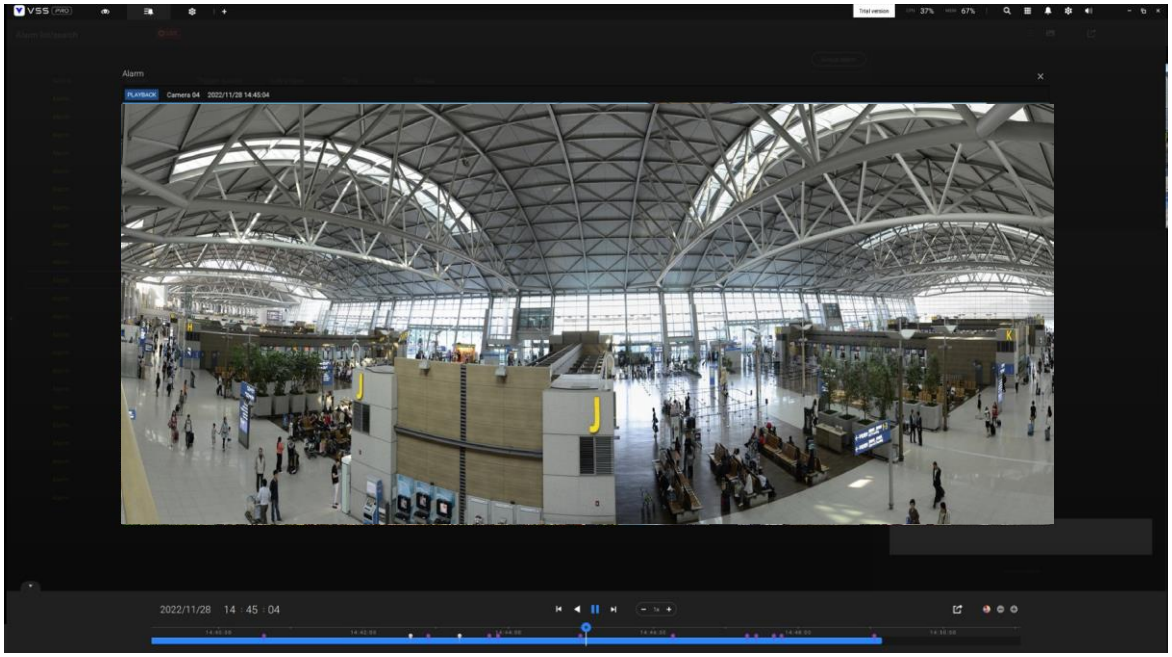
You can use the Export button to export a full list of all triggered events into a CSV file.
The event type, receiving station, triggering device, time of occurrence, and event status will all be listed.
You can also export alarm-triggered videos.

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

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

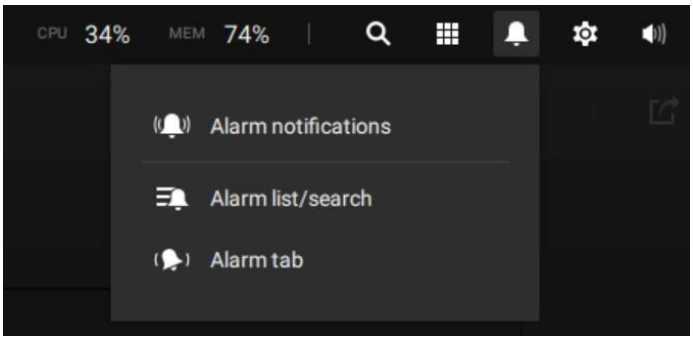


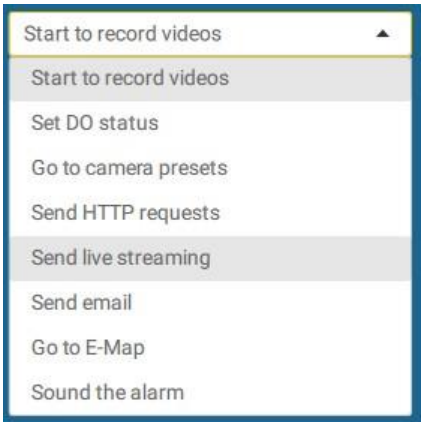
Double-click on the small playback screen again to bring it to the full view. The playback control, timeline, export, and alarm tags will be available on the screen.



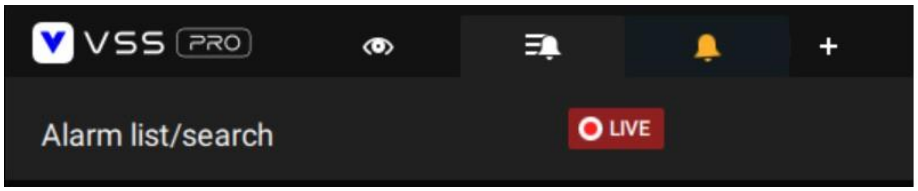
Alarm tab

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.

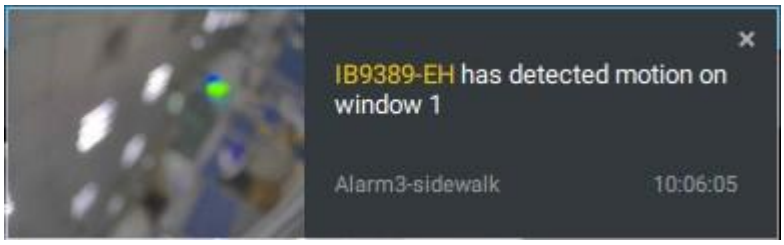




When a live streaming is sent by an alarm, an orange ringing bell icon will display.



An alarm prompt will also display on the screen.



You can click on the ringing bell icon to open the Alarm tab window. The alarm-trigged streaming 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)
	24		

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 thumbnail			Enter
Back to Thumbnail page			Esc
Next Thumbnail			Arrow right
Previous Thumbnail			Arrow left
E-map 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.

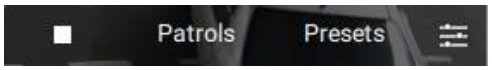
2. **Fisheye** cameras:  Fisheye display mode - Snapshot - Thumbnail search - Smart search - Replay.

   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 the 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 71.

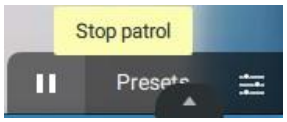
To exert PTZ control, first click on this button  to enable PTZ control.

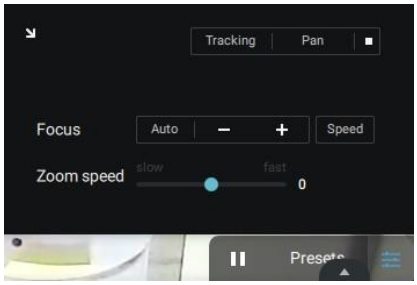
When PTZ control is enabled, the following controls are available on the



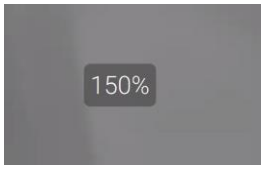
screen:

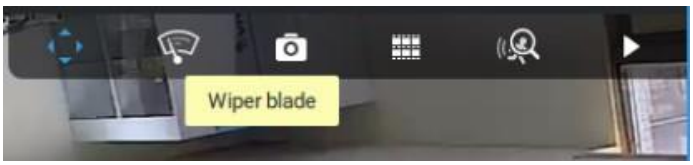
Click Patrols or Presets if these have been configured on the PTZ camera. You will need to open a web console to the camera to configure preset positions.





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 toolbar.

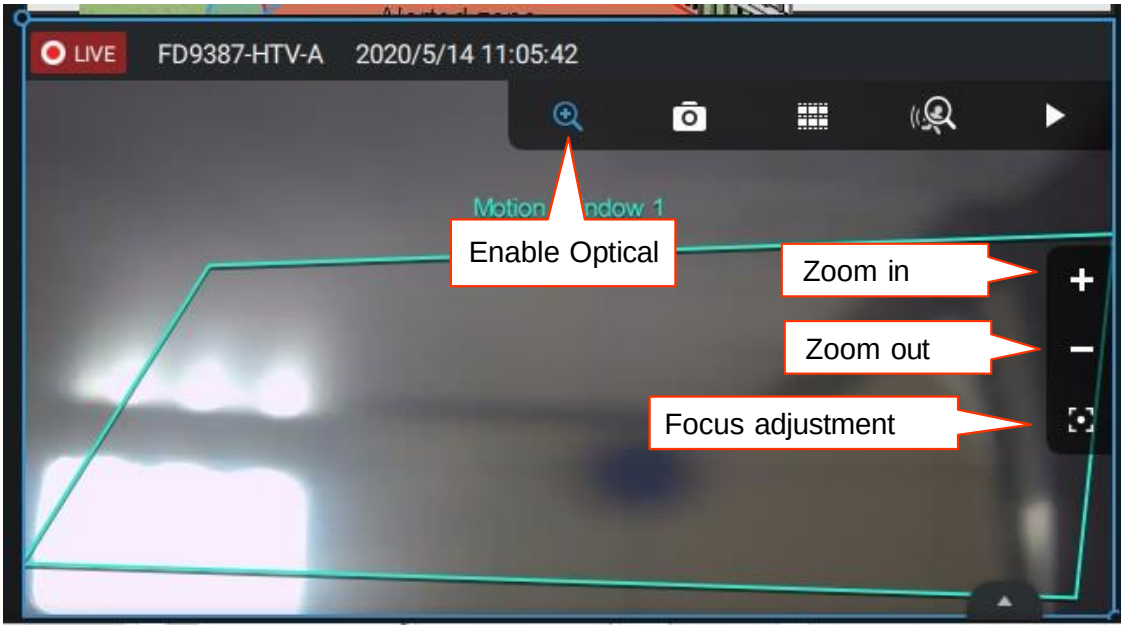
You can use the mouse wheel to zoom in or zoom out on the screen. The zoom ratio is shown on the screen for half a second.

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.

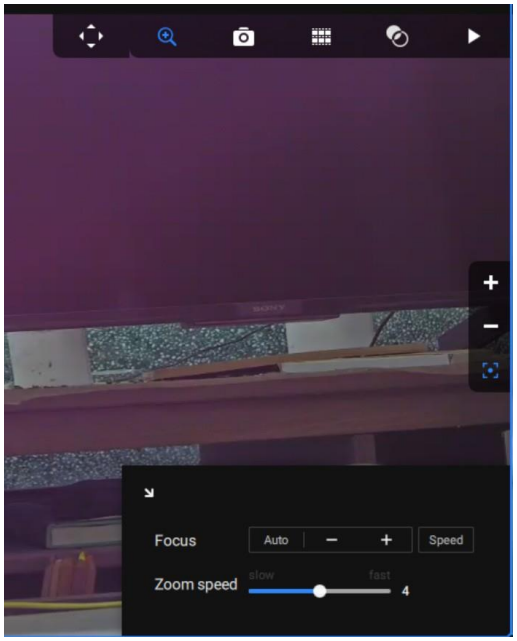
3. **Motorized lens** cameras:  Enable Optical - Snapshot - Thumbnail search - Smart search - Replay.

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



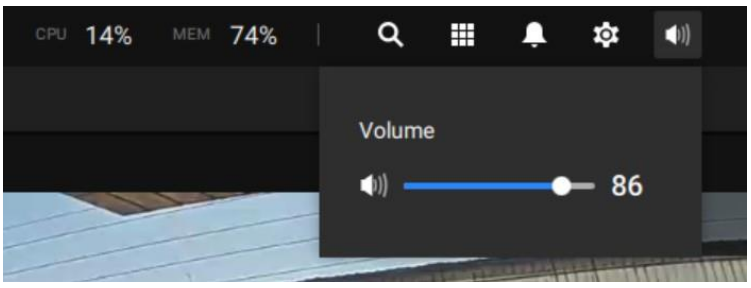
Click on the Focus adjustment button to bring out the focus panel. If you find the image is out of focus, you can use the +, -, or Auto buttons to regain the best image focus.

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



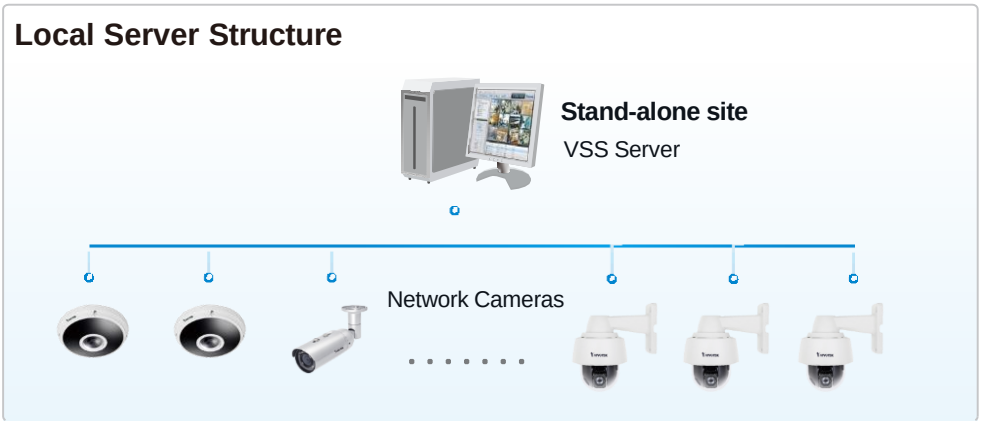
Audio

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



Server and Client Components

VSS Server provides a centralized management site for video recording. Users can log in 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.

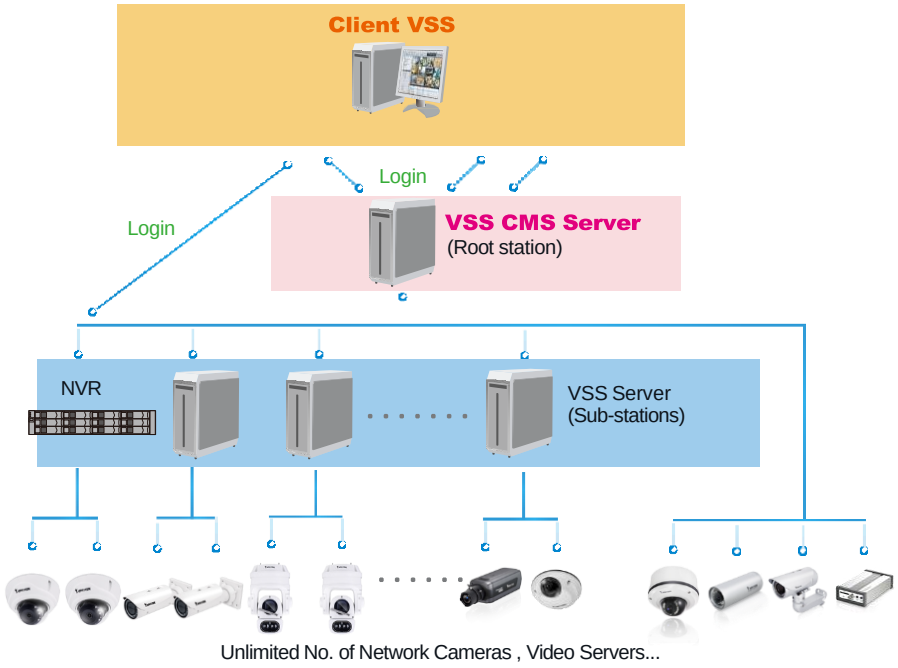


For users who manage large-scale surveillance deployments, please plan the hierarchical structure first. Then you can start to add cameras to each station and connect these sub-stations to the root station. The whole hierarchical management system is thus constructed. VIVOTEK's NVR stations can also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

Multiple Server Applications

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

Remote Server Structure



Please refer to the Stations page for how to enlist VSS sub-stations.

Chapter 2: Starting Up

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

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

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

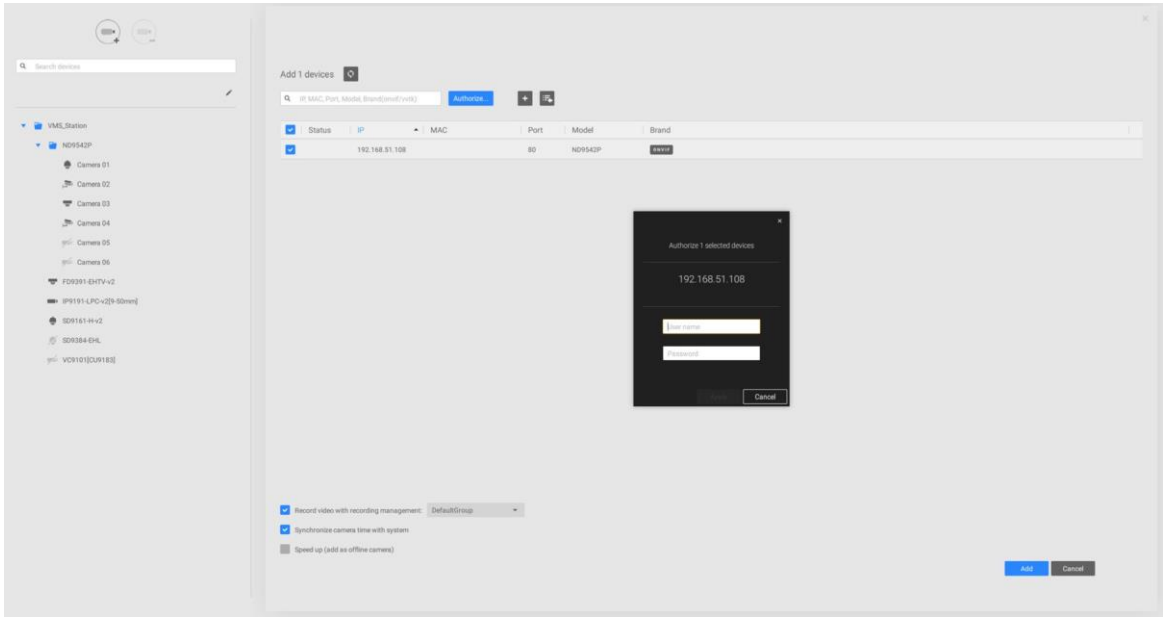
Use the Add device button to manually add a camera with its known IP or domain name.

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

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

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

Use the Refresh button to search the local network again.



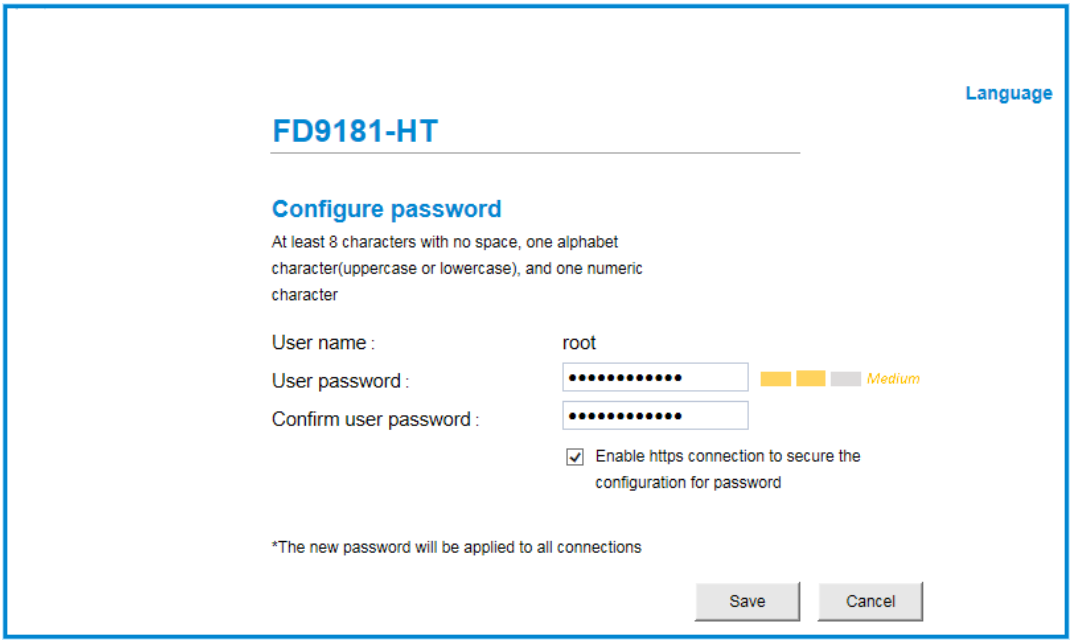
2-1. Selecting Devices

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:

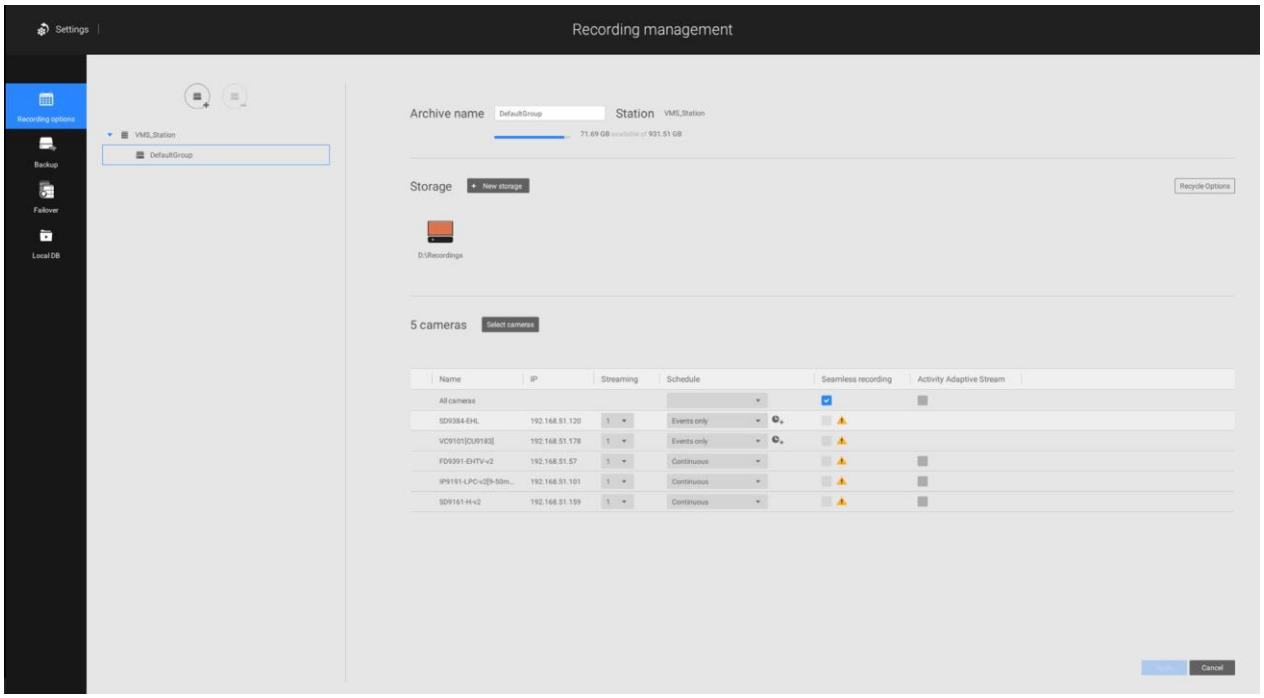
For cameras that come without password protection, you should open the Shepherd utility to locate and open a web console and configure a password for protecting the access to the camera. If a brand new camera (with no password) is selected for your VSS configuration, it will join your configuration without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



2-2. Recording Options

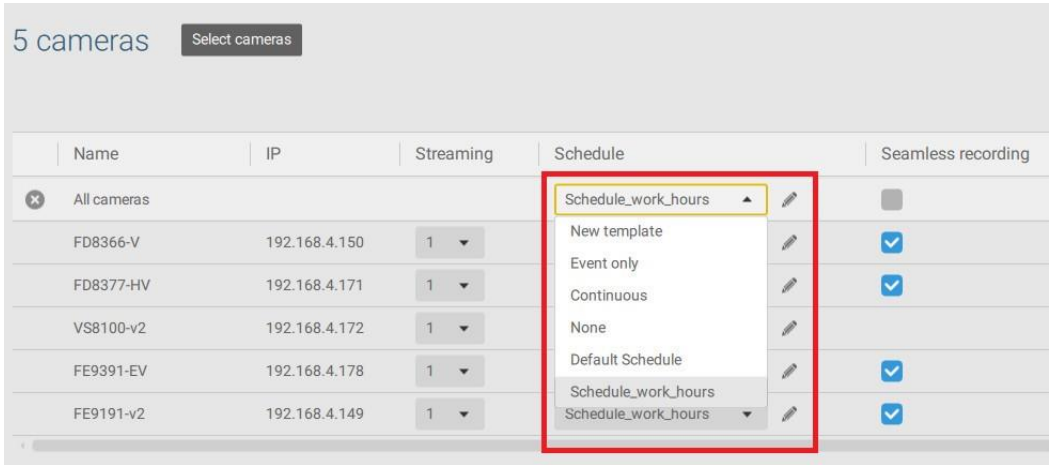
Click **Settings** > **Recording** > **Recording options**. The Recording options window will prompt.

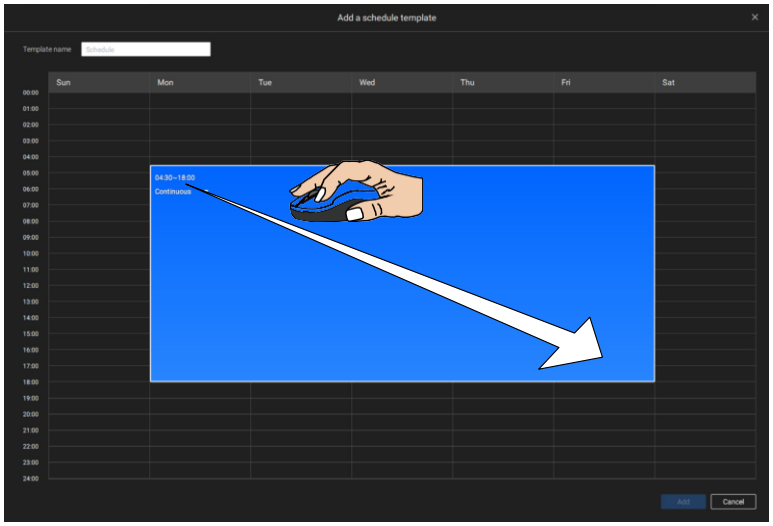
You can configure recording schedules or select the storage options, including the configuration of an external NAS storage.



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

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



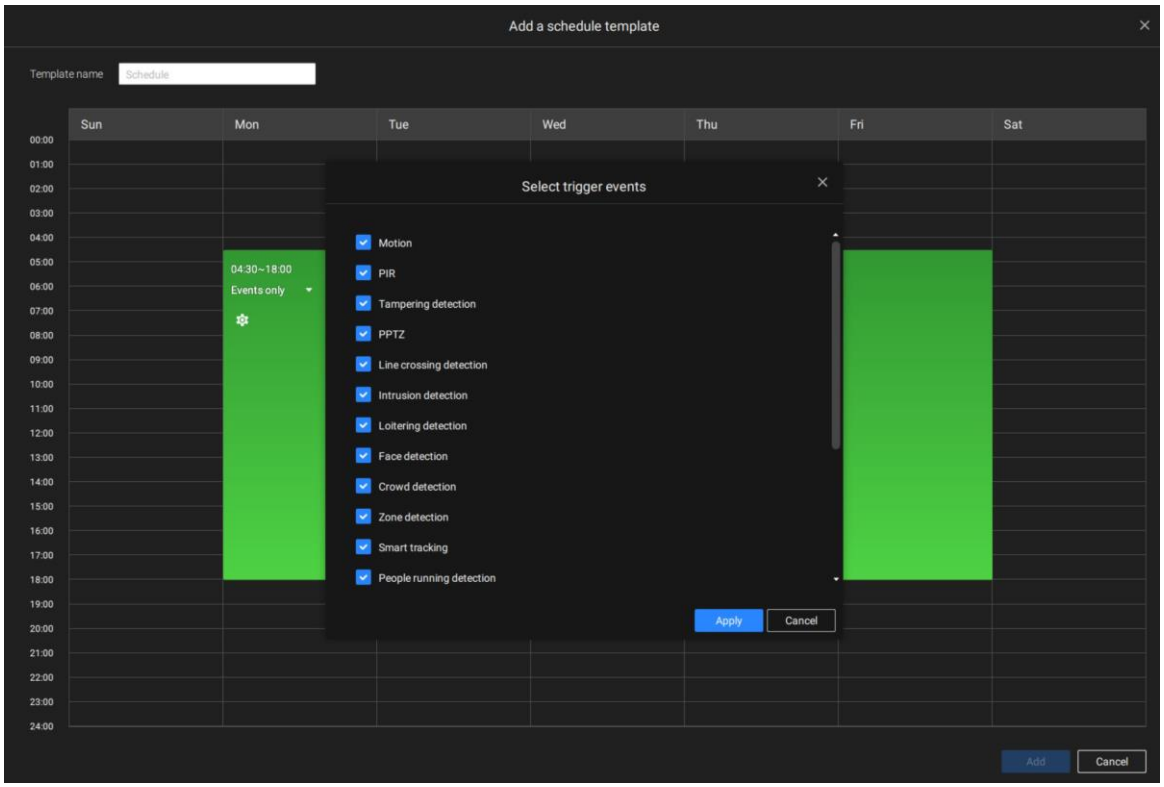


Click and hold down on the time cells, and drag the mouse to include the time span of your preference. The minimum selectable unit is half an hour. You can select separate and multiple time spans on the template.

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

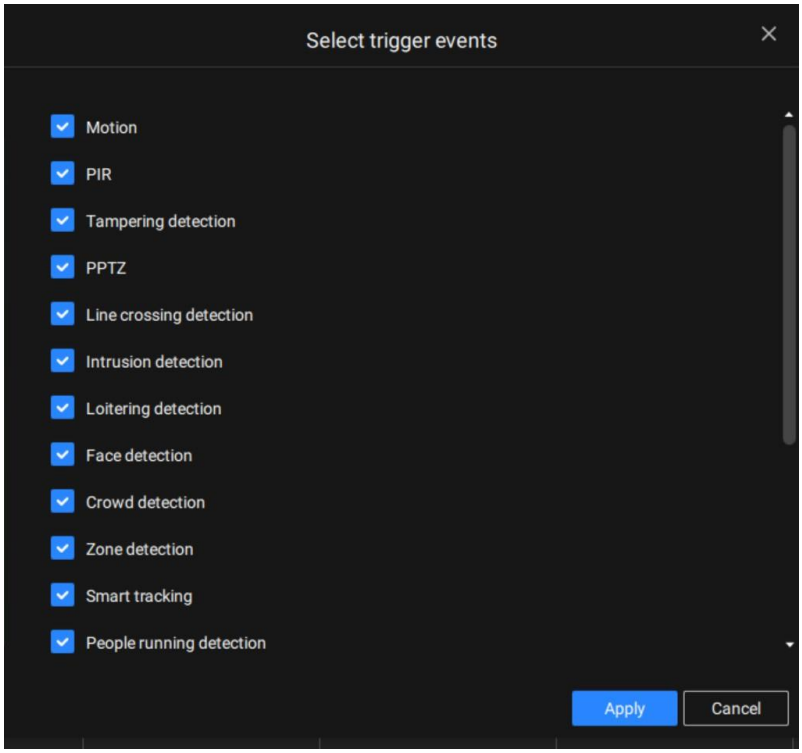
The same configuration window applies to both the Schedule template and the customize schedule windows.

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

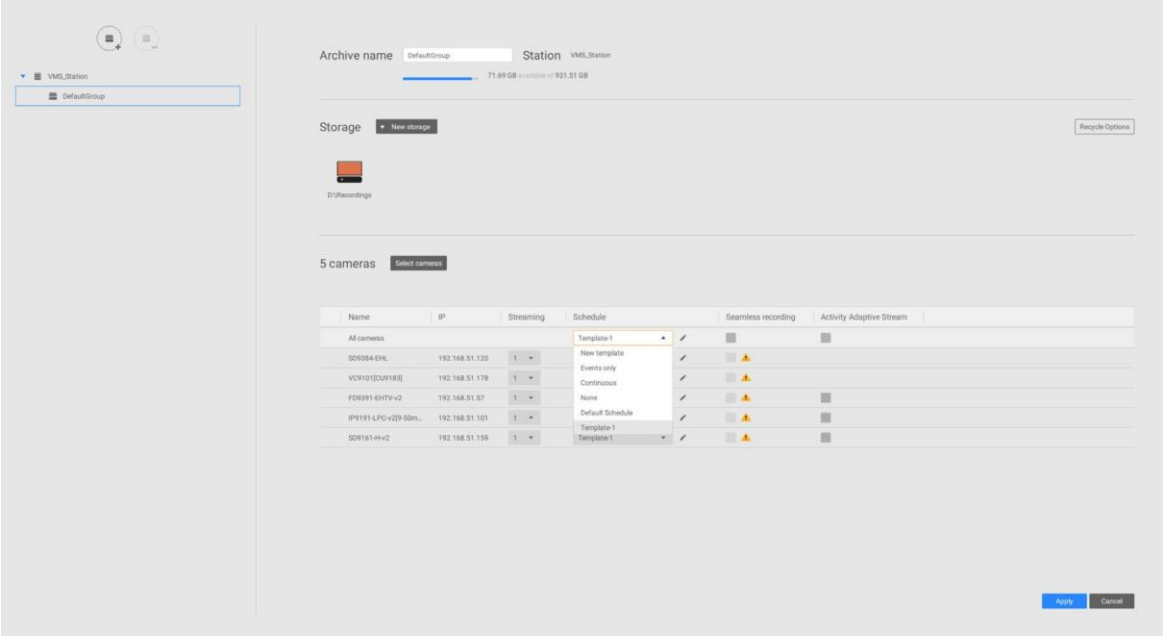


When Events only is selected, click on the Settings button to proceed.

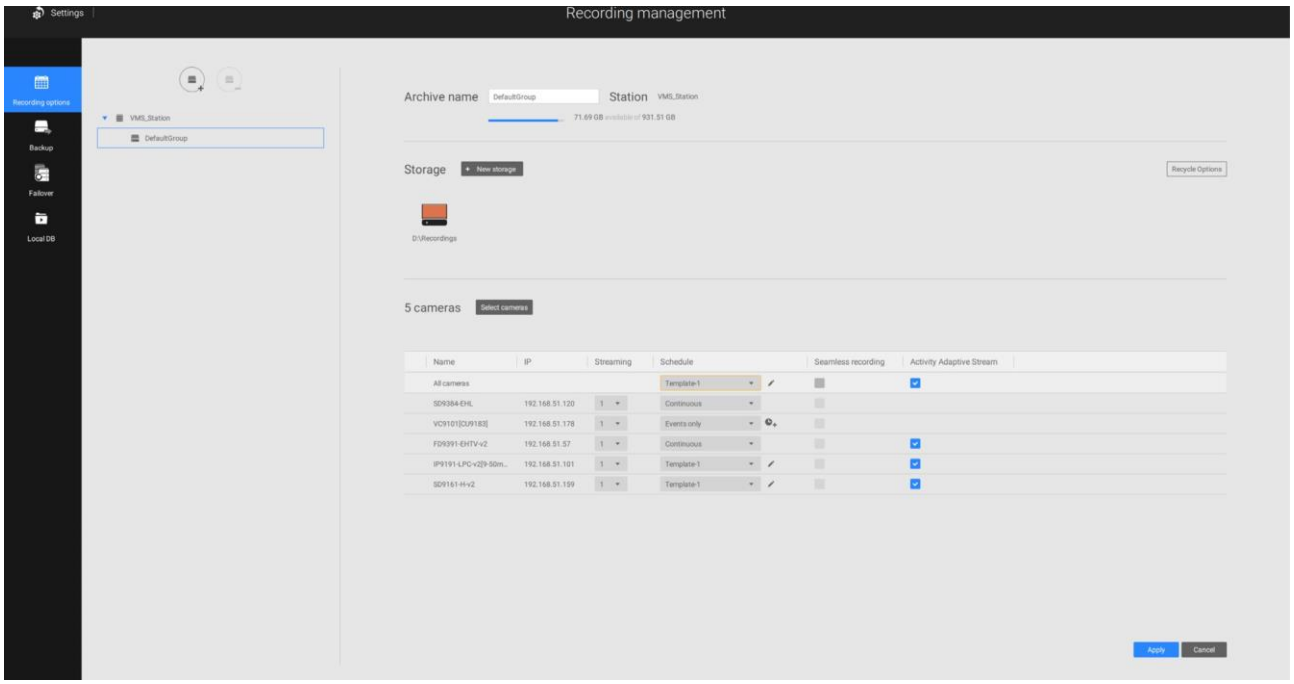
The applicable event types will be listed. Select the types of event triggers that you prefer. Click **Apply** to leave this page. By default, all applicable event triggers will be selected.



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

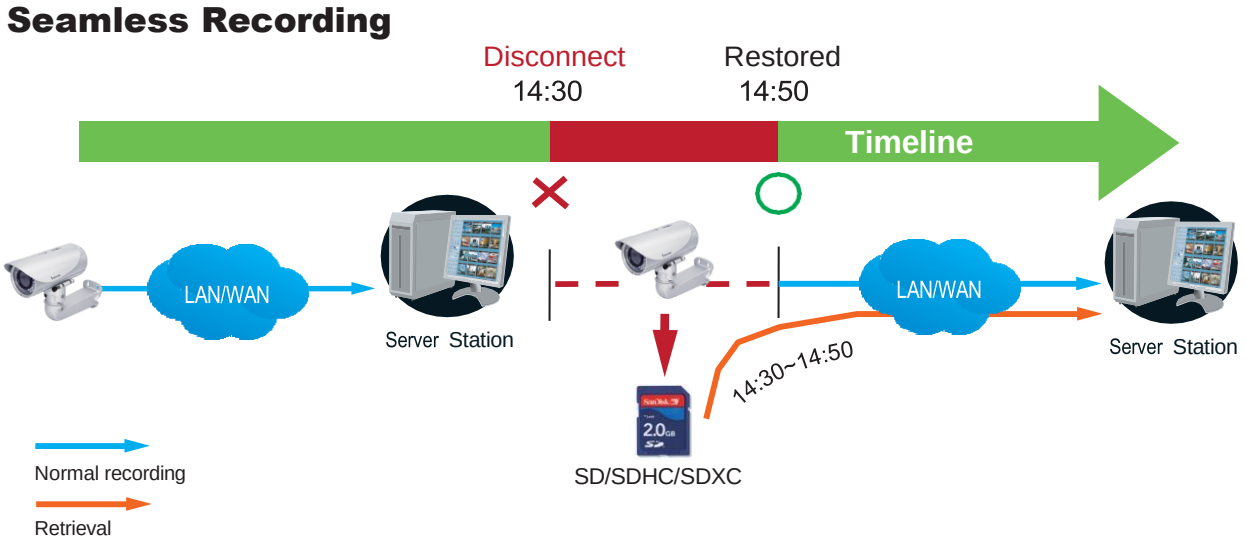


Make sure a Schedule mode is selected when you leave this configuration step.



Seamless Recording

Seamless Recording safeguards critical videos in the occurrences 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 VSS server can automatically resume the recording. More remarkable is that, a VSS 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.

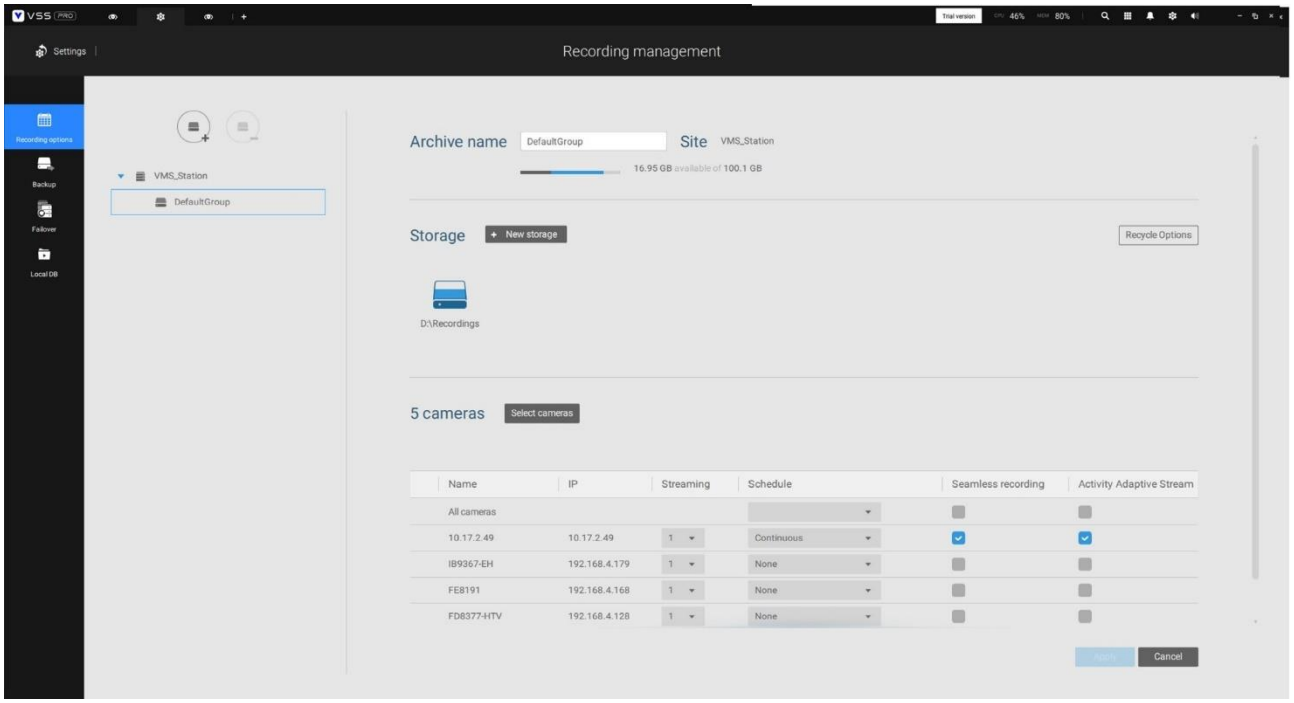


The video data retrieved from SD/SDHC/SDXC card also include event-triggered recordings such as pre- or post-event footages, if events were detected during the network outage.

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.

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.



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:

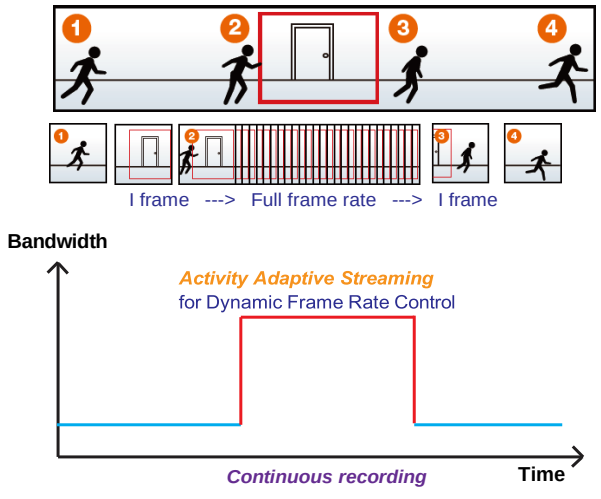
■ Pre-event recording and post-event recording
The Network Camera has a buffer that temporarily holds data for a period of time. Therefore, when an event occurs, the camera can retrieve image frames taken several seconds ago. Enter a number to define the duration of recording before and after a trigger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

■ Priority: Select the relative importance of this recording (High, Normal, or Low).

■ Source: Select a video stream as the recording source.

NOTE:

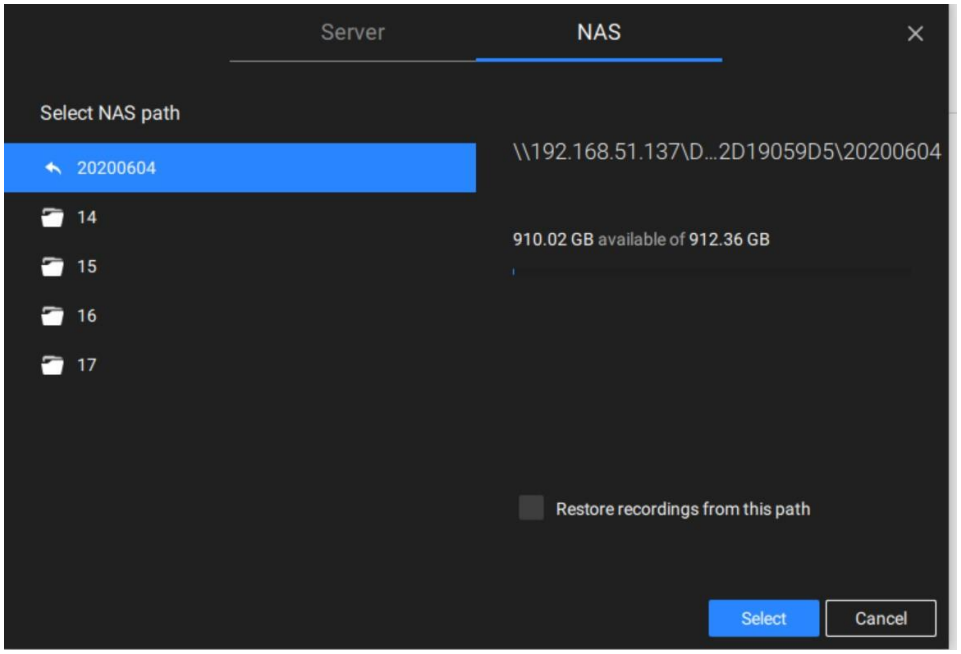
* To enable adaptive recording, please make sure you have configured the trigger sources such as Motion Detection, DI input, or Manual trigger.
* When there is no alarm trigger:
  - JPEG mode: record 1 frame per second.
  - H.264 mode: record the I frame only.
* When the I frame period is > 1 second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



2-3. Storage

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

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



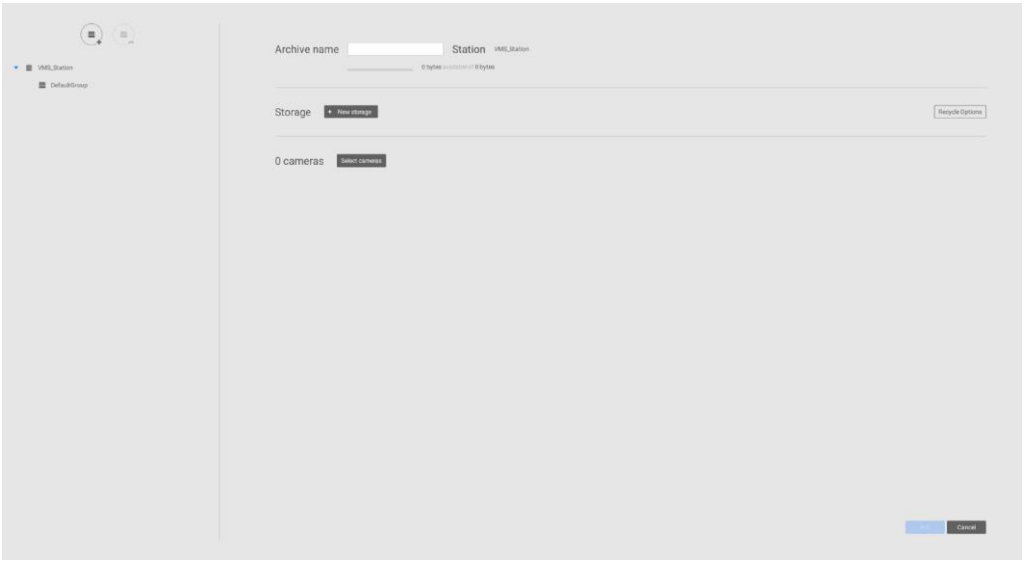
Select storage volumes each by a single click.

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

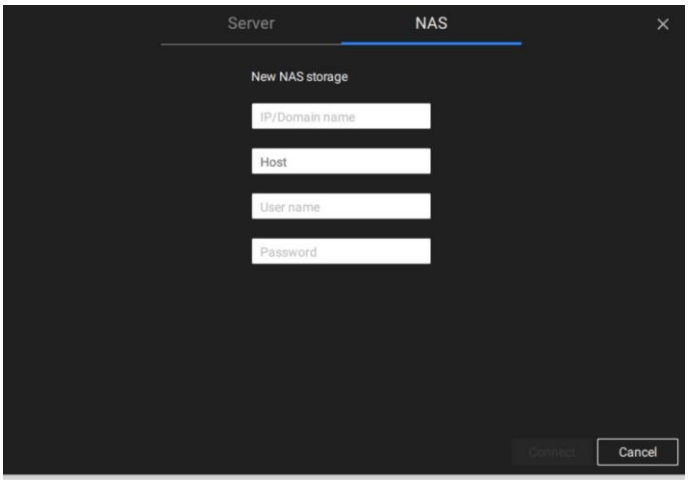
Adding NAS (Network Attached Storage) as a Storage Option

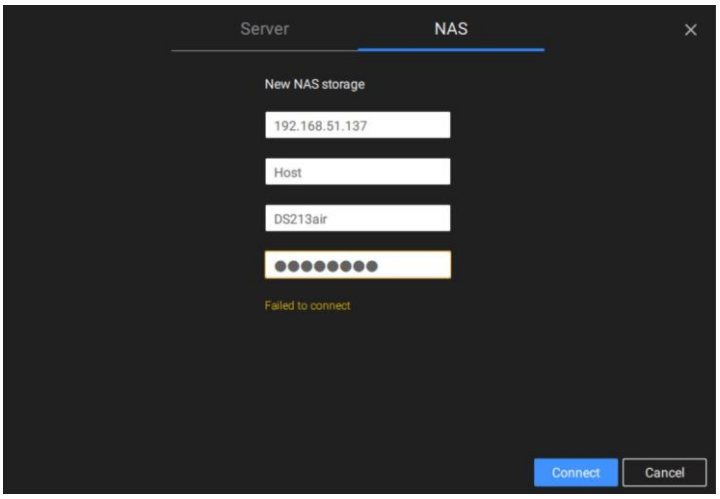
You can also record videos to a networked storage.

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



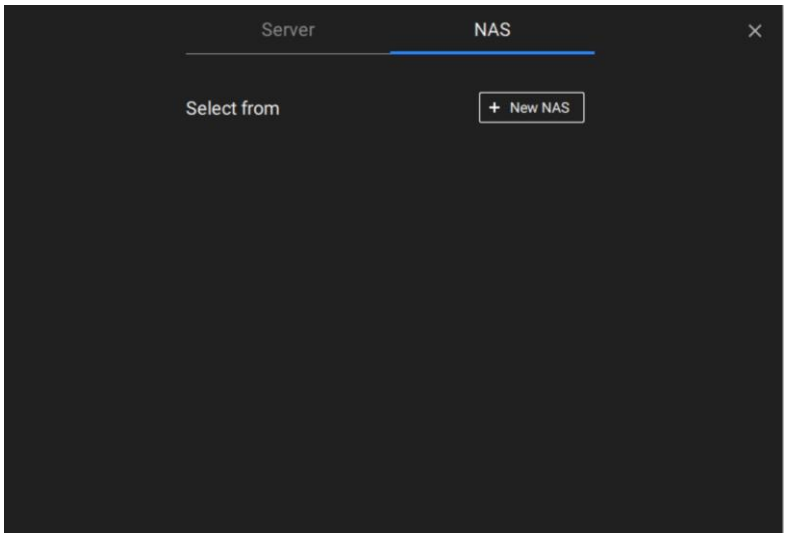
4. Click the + New NAS button.



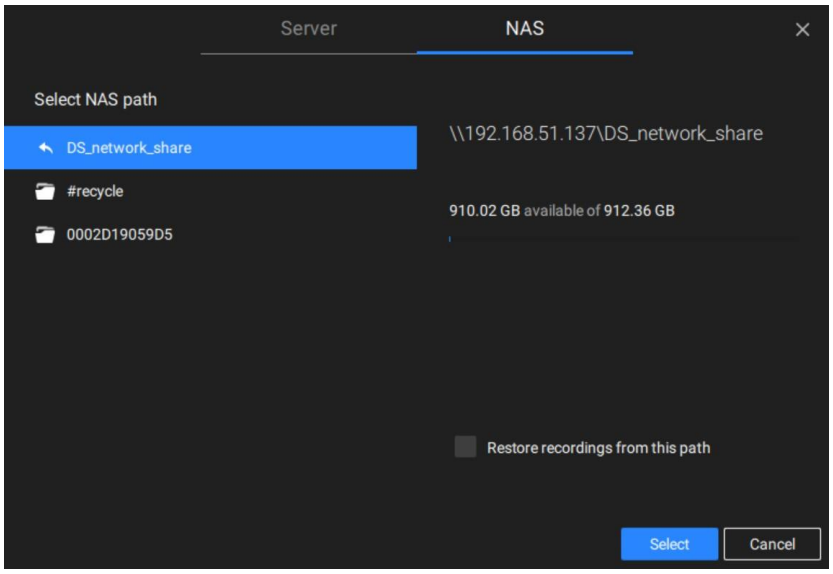


5. Enter the NAS storage's address and the credentials for access to the networked storage. When done, click the **Connect** button.

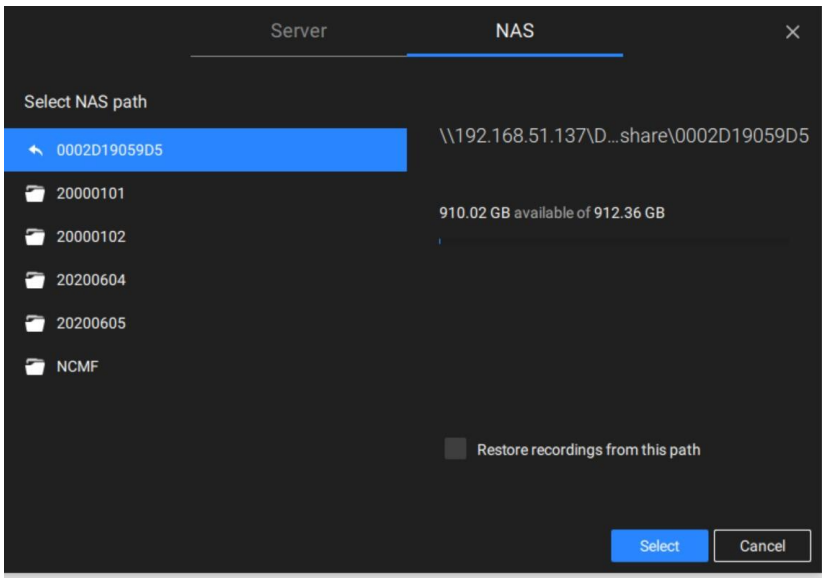
6. The NAS storage should appear on screen. The connection may take several seconds. Single-click on the NAS storage to select its network shares.



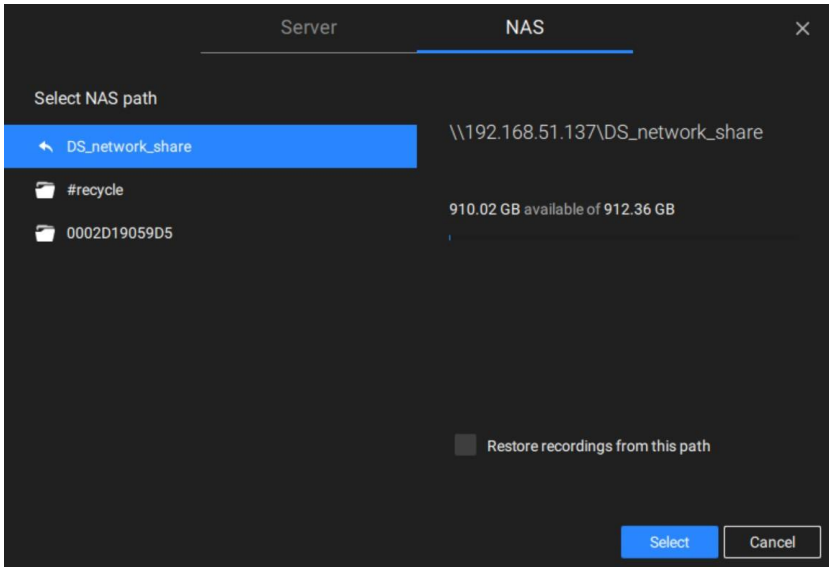
7. The NAS storage's network shares should be listed. Single-click to select a network share.



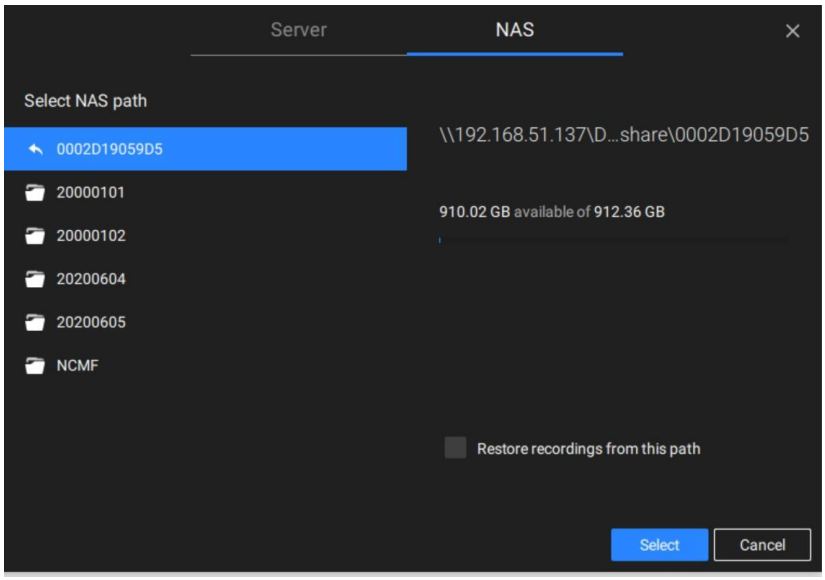
8. Click **Select** when done. Note that you can repeat the previous process to select multiple network shares from a single NAS storage.



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

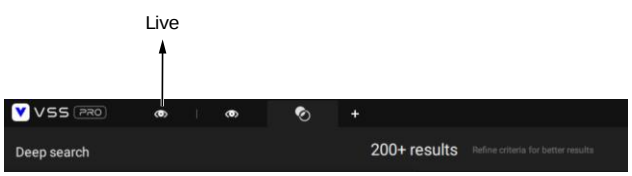


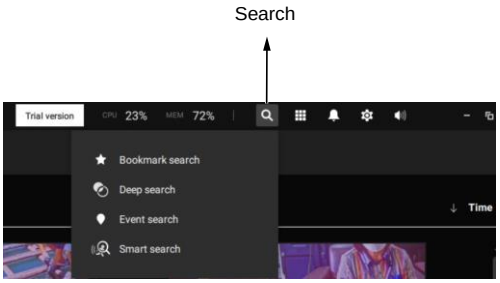
10. Click **Select** when done. Note that you can repeat the previous process to select multiple network shares from a single NAS storage.



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 startup, 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.

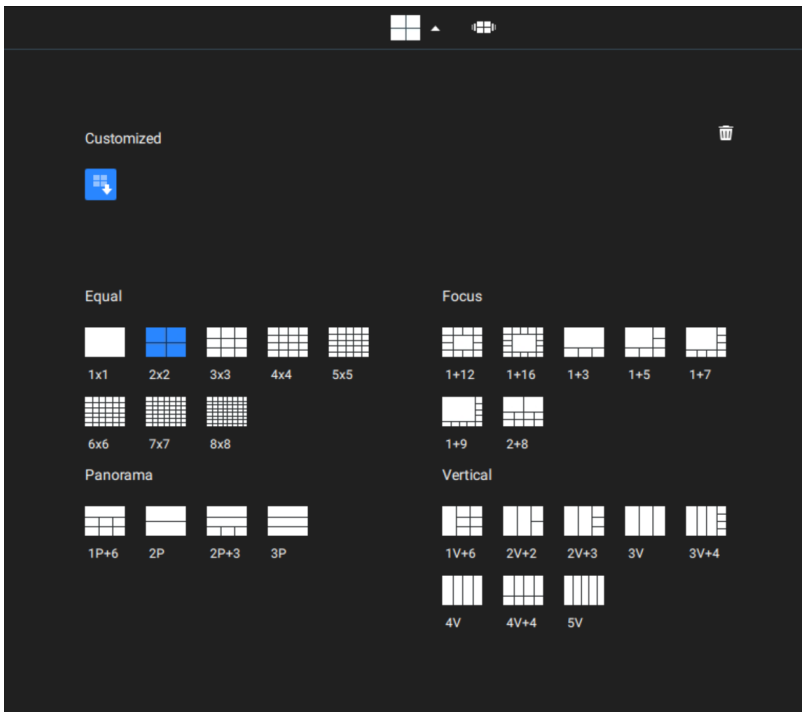
The available layouts are categorized into 4 types: Equal, Panorama, Focus, and Vertical.

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.

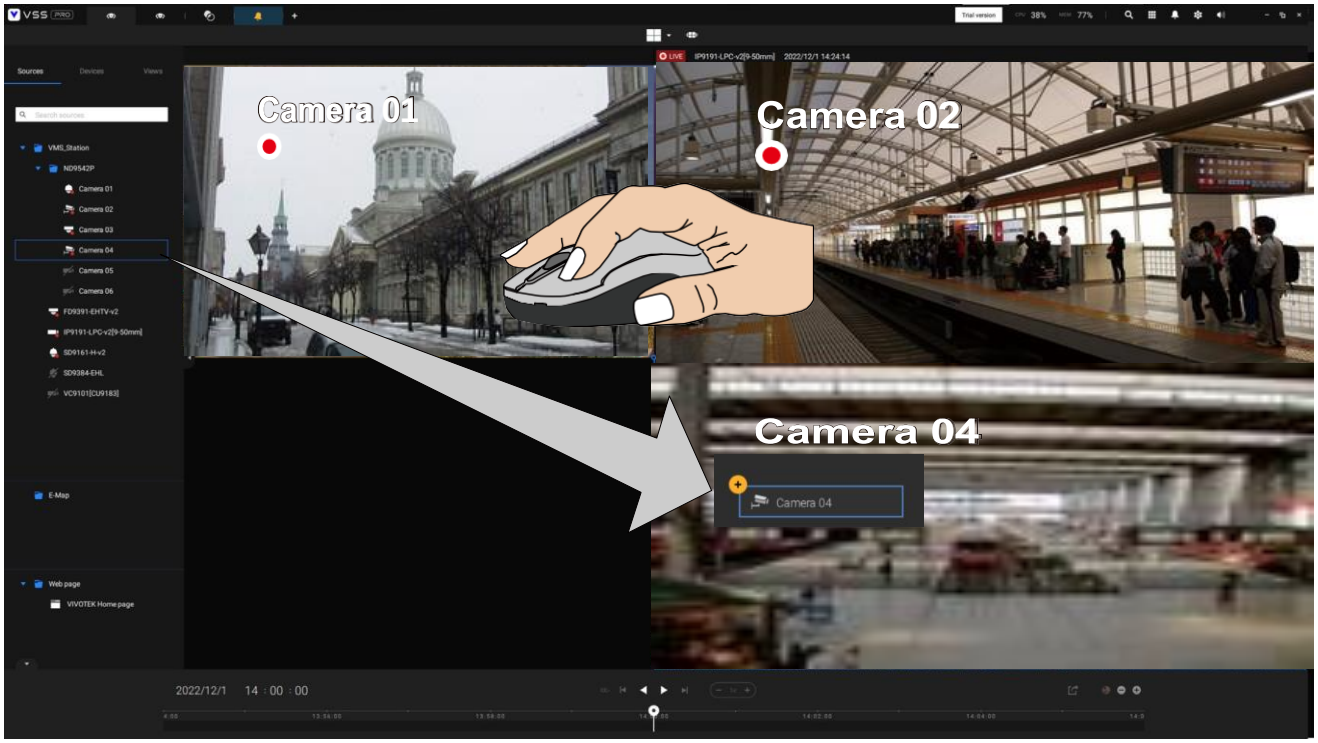
Vertical: 1V+6, 2V+2, 2V+3, 3V, 3V+4, 4V, 4V+4, 5V. (applies to corridor view)



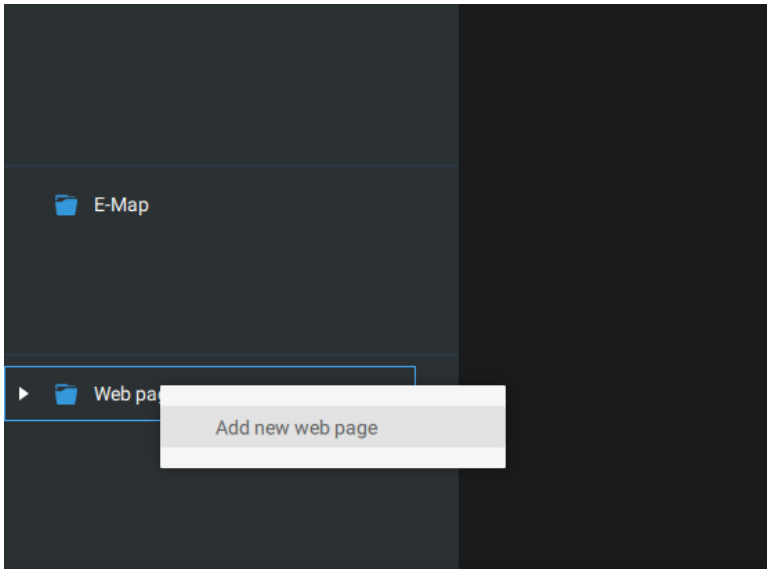
To design and customize a layout, please refer to the Customizable Layout page.

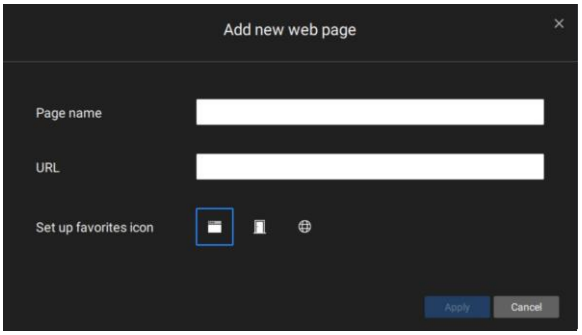
You can then fill in the view cells by dragging and dropping cameras into the view cells. While dragging, a name tag displays. All cameras should be listed under the VMS Station Device Group.

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.

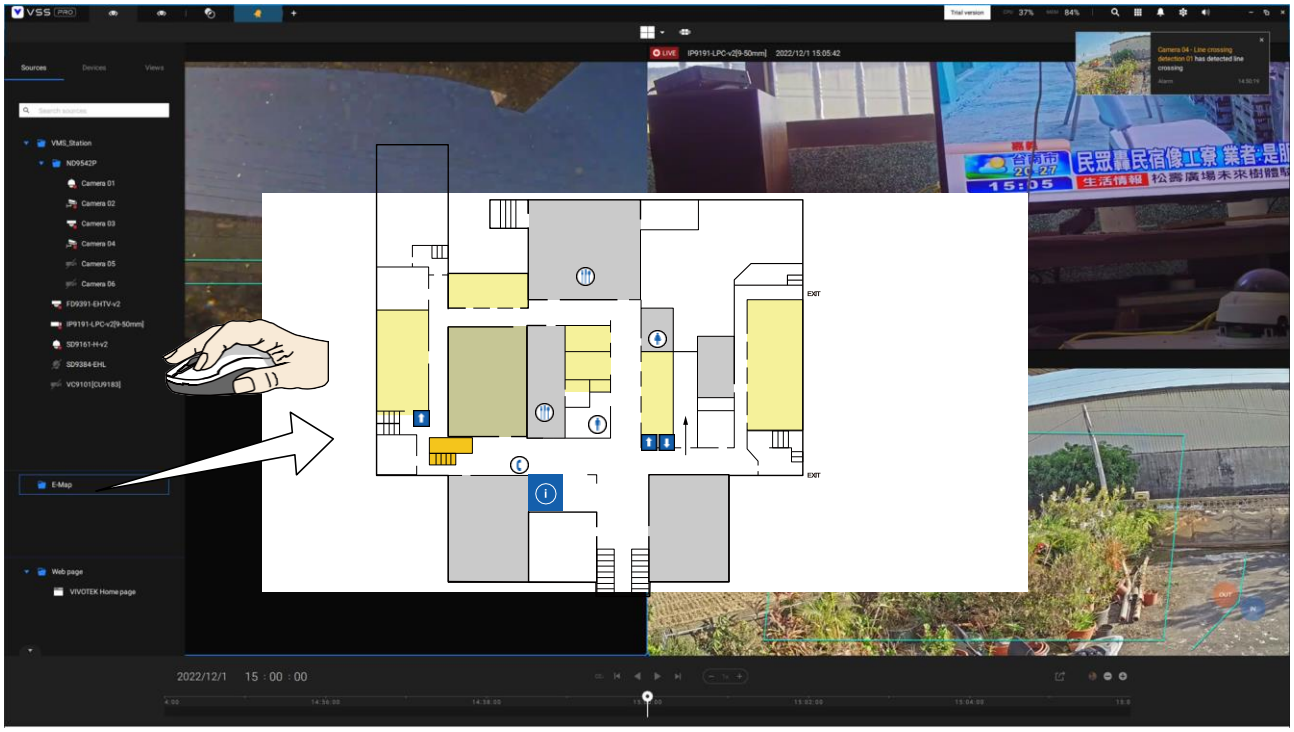




When configuring a web page to be displayed in view cell, you can select a favorite icon.

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

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

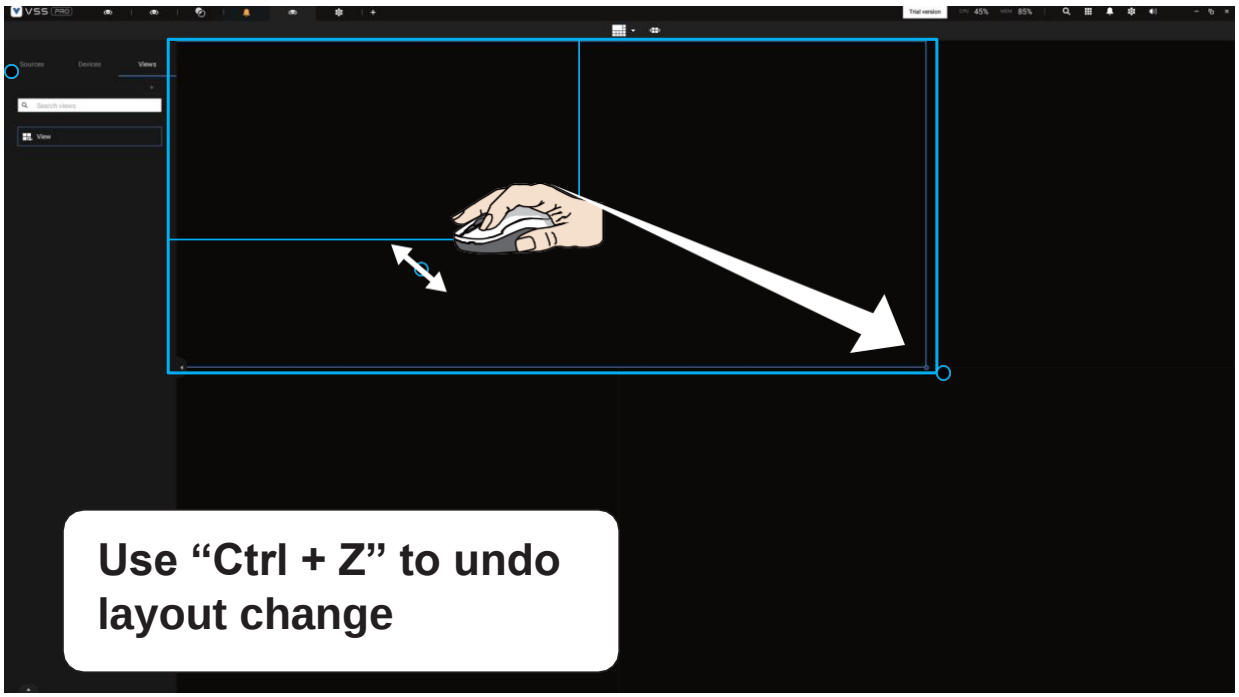


2-5. Customizable Layout

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.

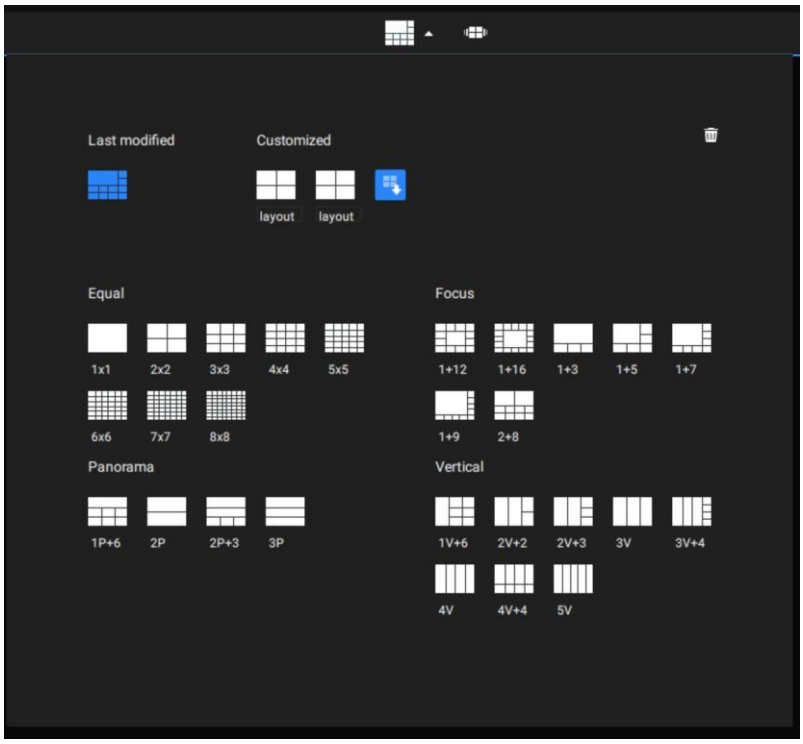
Click and drag the corner mark on a view cell. Drag across the screen and release the mouse button to enlarge the view cell. Choose a standard layout of many view cells, e.g., 7x7 or 8x8, if you want to design a complex customized layout. You can create a special layout, e.g., an especially wide view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

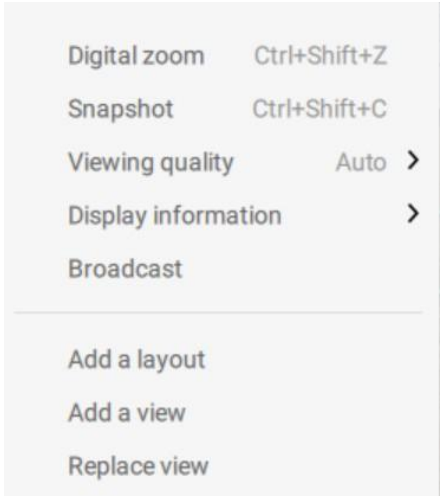
To abandon a customized layout, simply select a new layout from the layout window. You can also use the Ctrl + Z keys to undo your changes on the layout.



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 double-clicking on its name.

To remove a configured layout, drag it to the garbage can icon on the upper right.





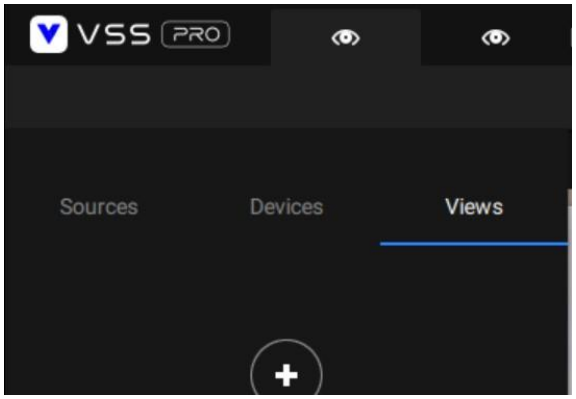
You can also right-click on the screen to display the **Add layout** option.
You can then click Device Group, and start filling your customized layout with camera views. When done, click **Add a view**.

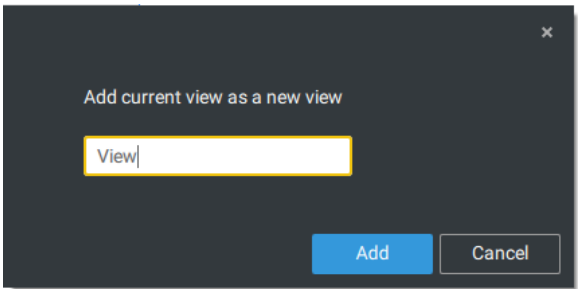
Also remember to save the current layout as a view, and save your configuration in **Settings** > **Preferences**.

2-6. Saving a View

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

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

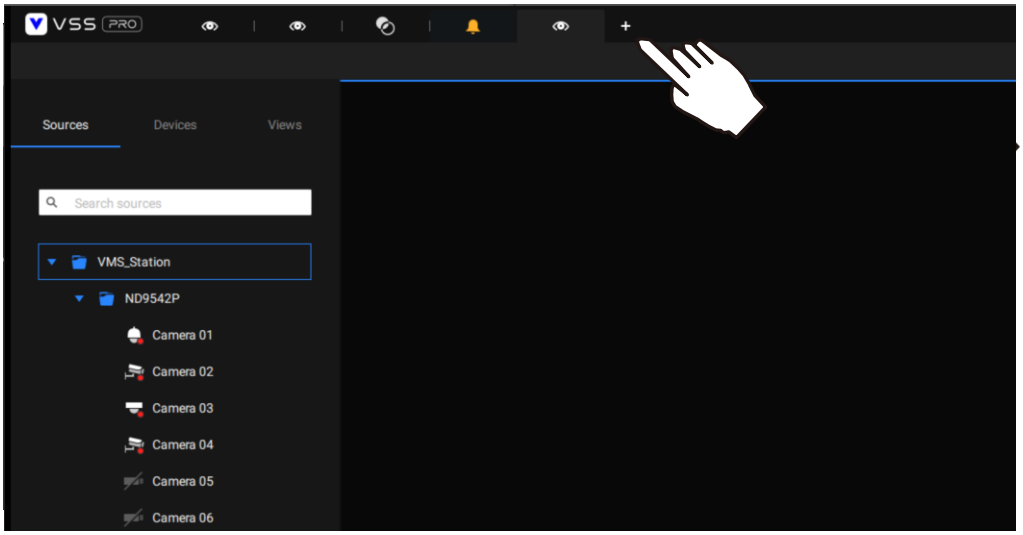




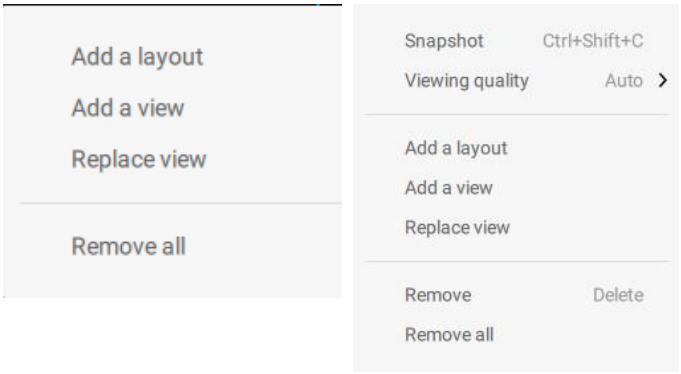
2-7. Add More Live Views

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

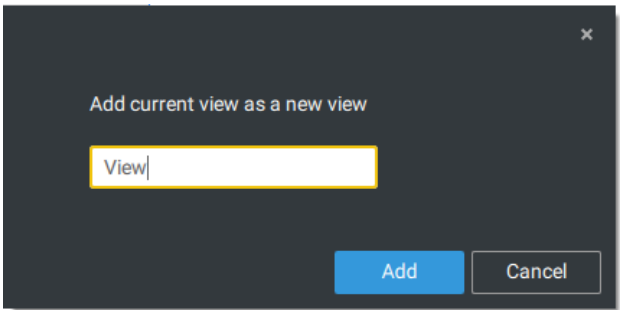
An empty live view will display, and you should repeat the above process to select a layout, and fill in the view cells. When done, save the view.



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

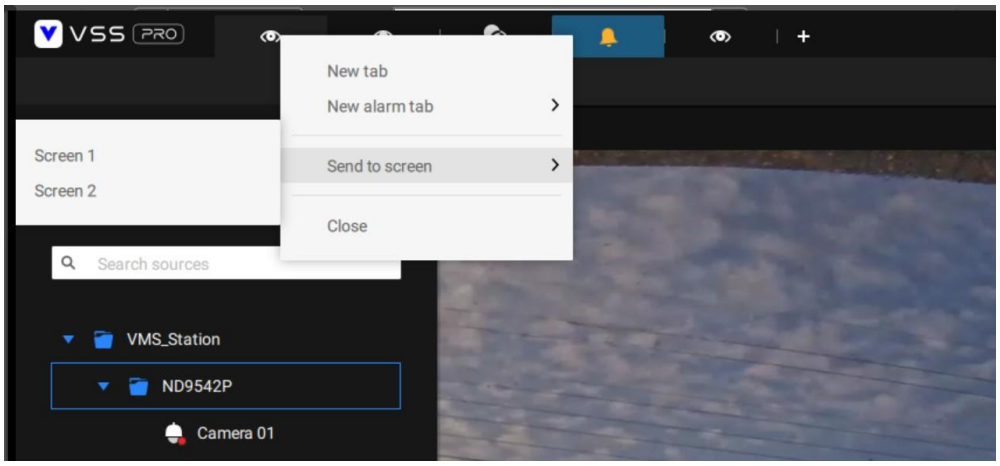


Enter a name for the new view and click **Add** to proceed. The new view will be listed in the View panel.



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.

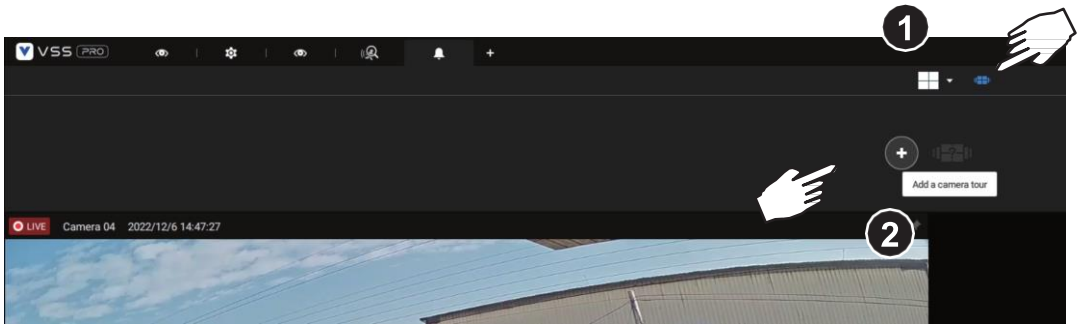


2-8. Tour

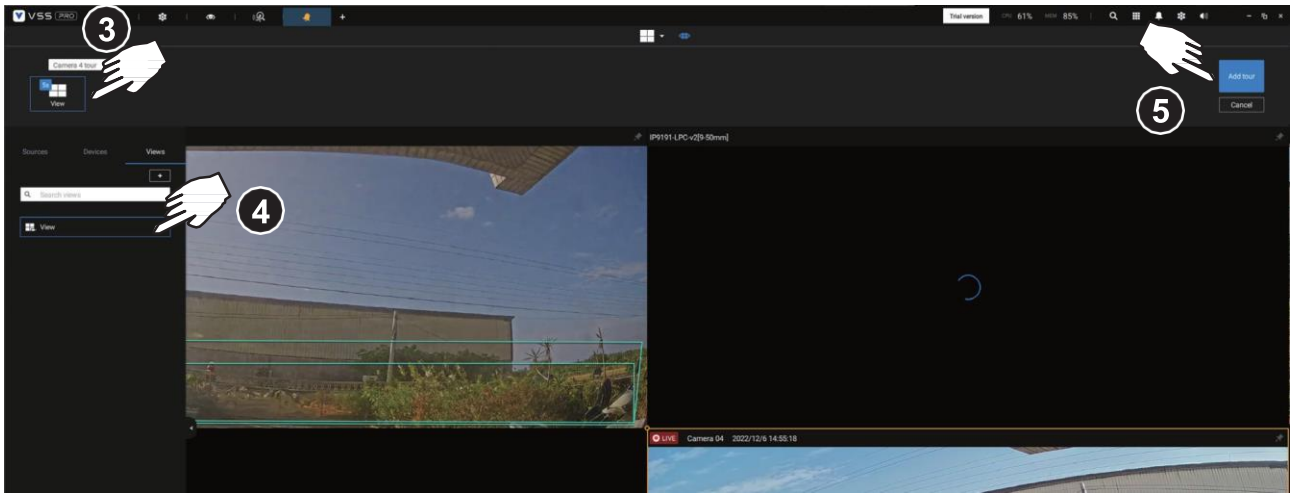
A tour can be configured to consecutively display multiple views. A tour allows users to quickly glimpse through many view cells in a timed pattern. As a tour can contain multiple views, you should design and configure camera views before configuring a tour.

To configure a tour,

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

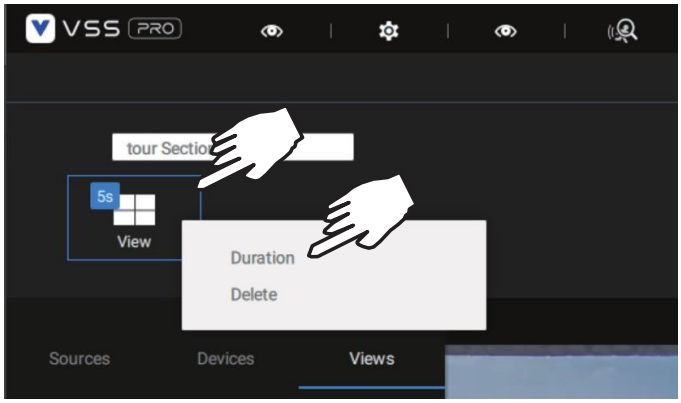


3. Enter a name for the tour.
4. Single-click to select a view. Select multiple views each by a single click.
5. Click the Add Tour button.

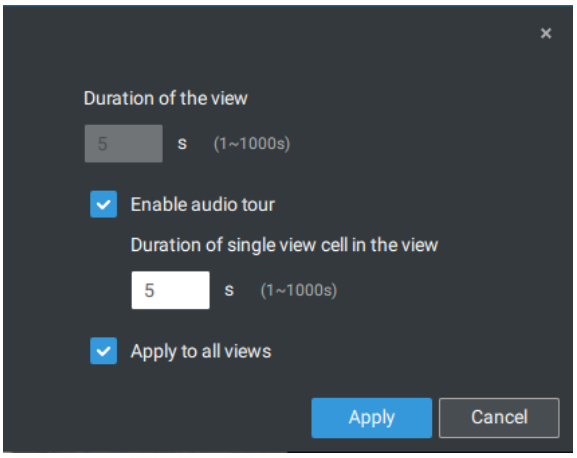


The default for the duration of the display of each view is 5 seconds. You can right-click on each view to display the Duration of each view. You can apply the same duration of all

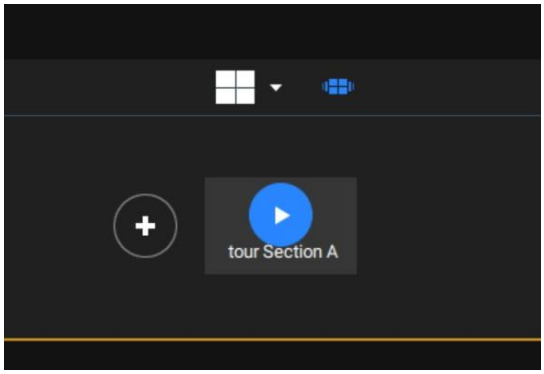
views, or allow each view to display on screen for a different span of time.



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



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



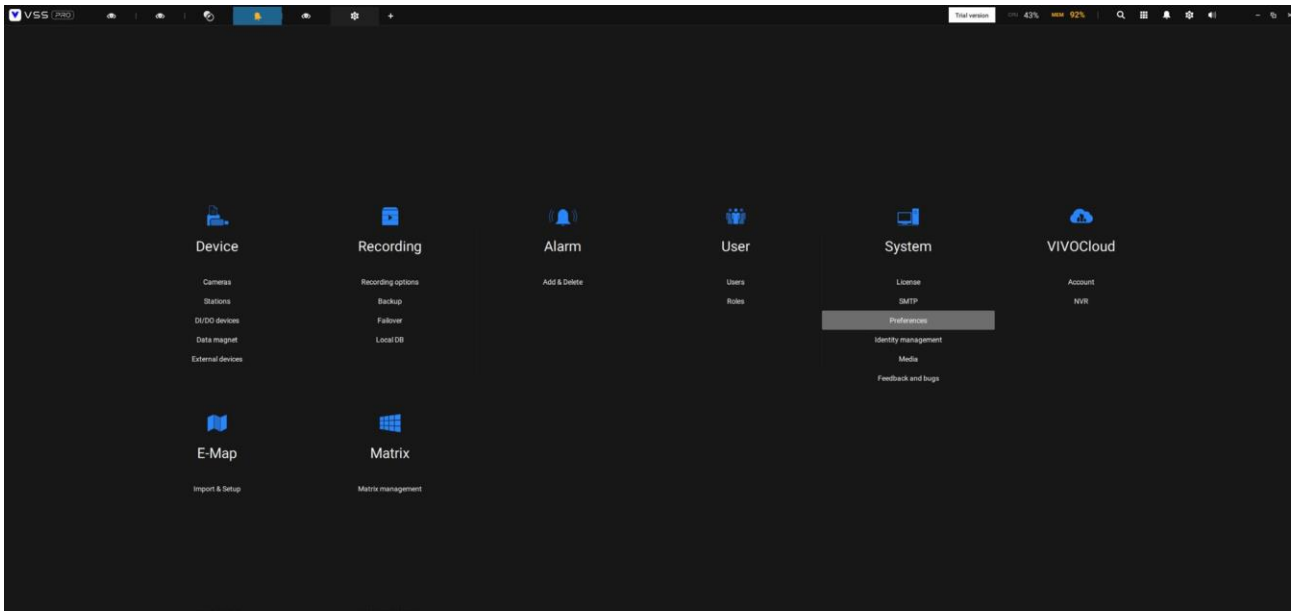
When playing a tour, and you want to stop the tour, you can left-click or right-click on the screen.

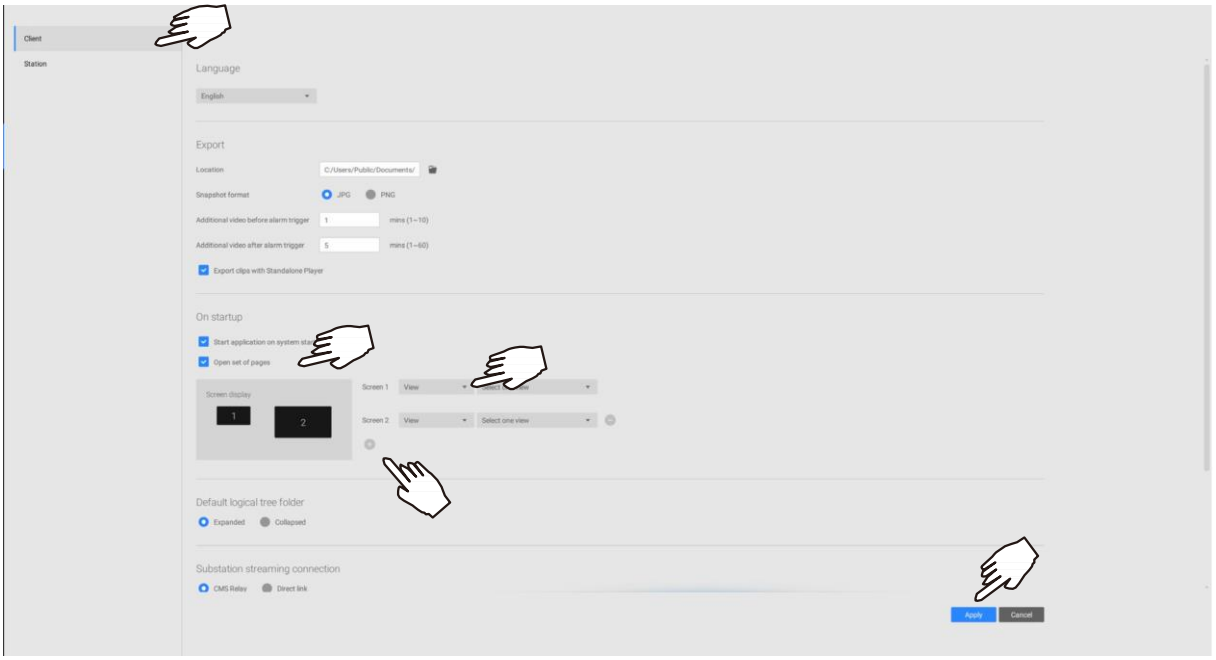
Click the Tour icon  again to return to the singular live view.

2-9. Save Your Preferences

Go to **Settings** > **System** > **Preferences** to save your current layout and display configurations.

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





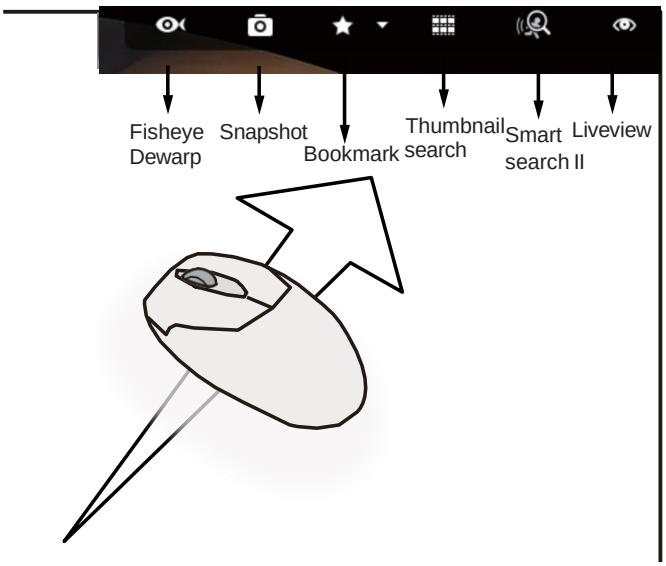
2-10. Playback

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, the 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:

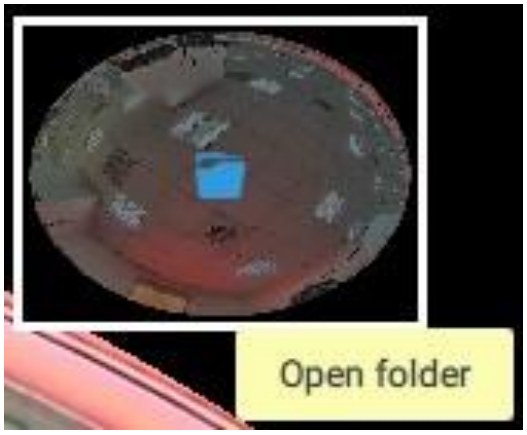
1. **Float Panel**: When Playback is started, swipe your mouse to the upper-right of the view cell to display the Playback float panel.



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.

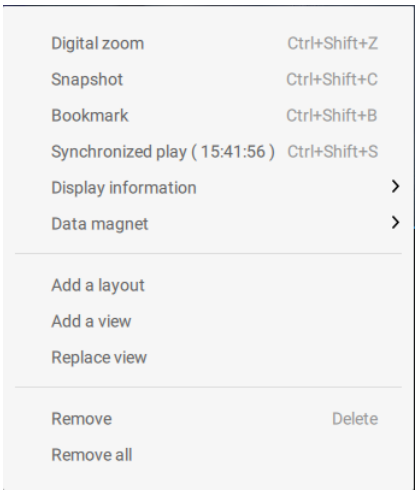


Bookmark: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos. Note that the bookmarked video clips are free from storage recycles. They will not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

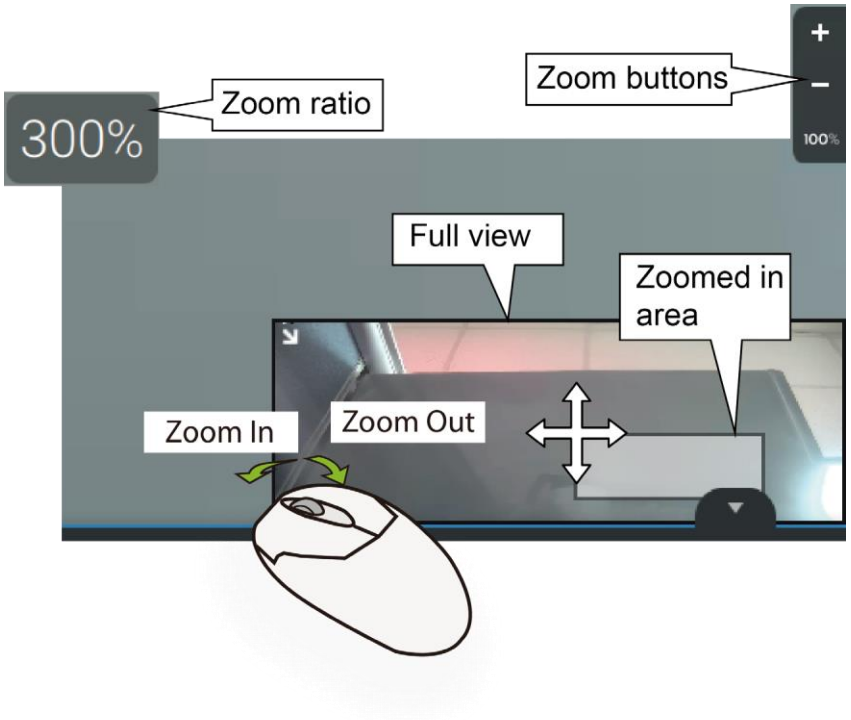
Smart search II: Smart search II is an independent function. Please refer to 2-19 Smart search for details.

Liveview: Click to return to Live view.

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



Digital zoom: enlarges an area by lowering image resolution (zoom in) or shrinks an area by increasing image resolution (zoom out).



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

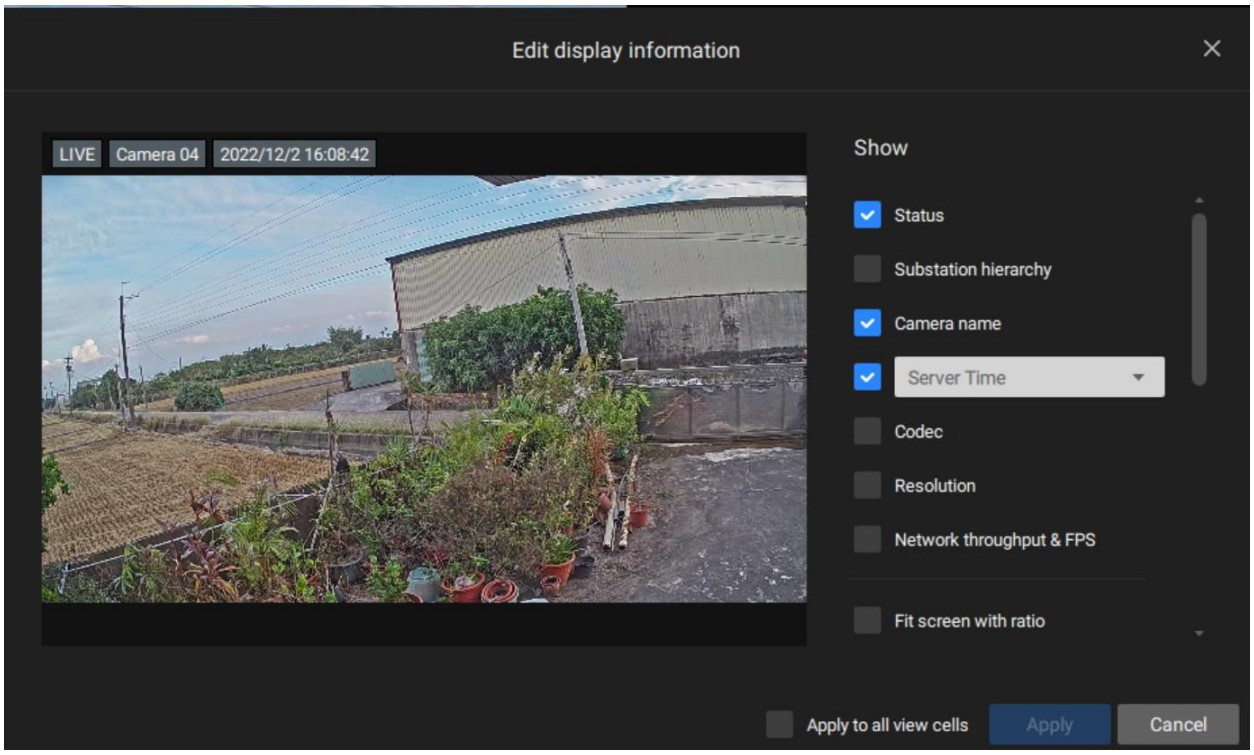
Bookmark: If you find anything of your interest when viewing the playback, click this button to create a bookmark. It helps when you need to return to the point in time after you review all through the recorded videos.

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

The following commands are general purpose commands.

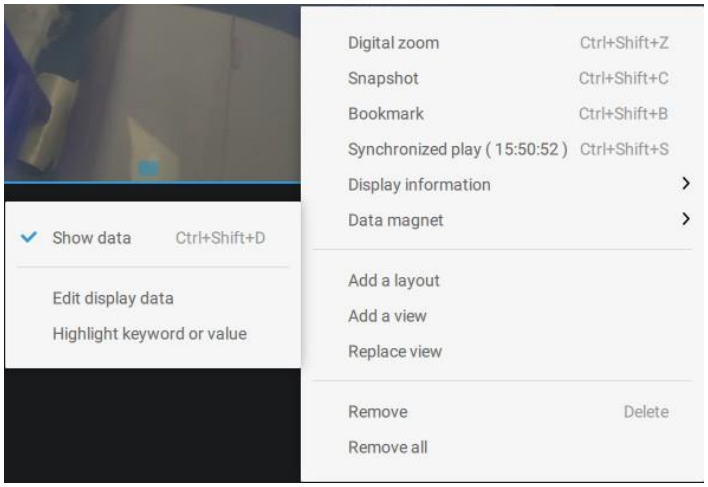
Display information: By default, all display elements will appear on screen for all playback windows. You can use the Edit display information to select more display elements.

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

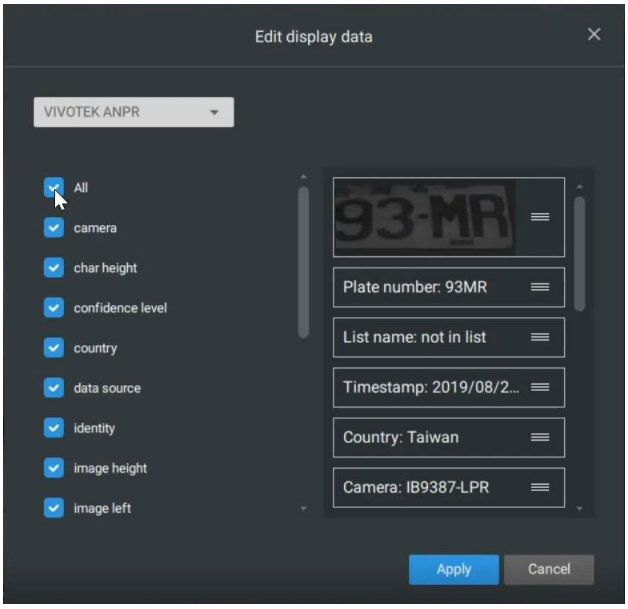


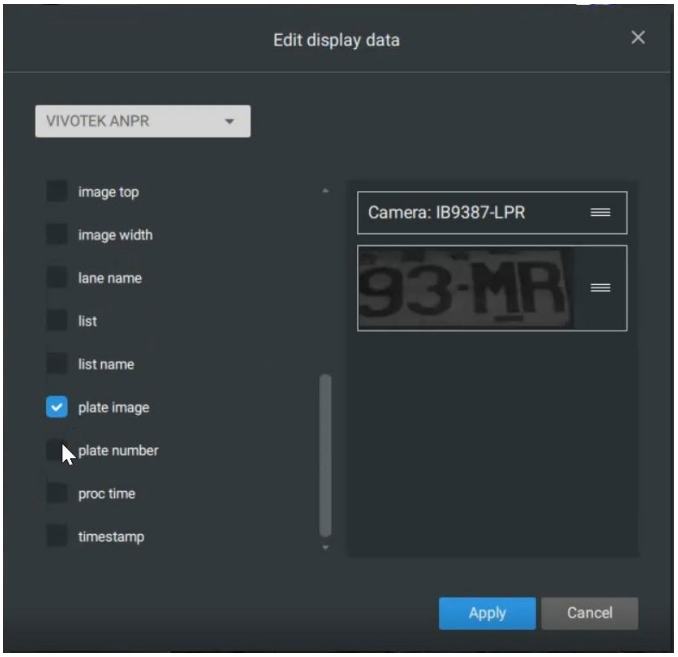
Data magnet: For 3rd-party applications, such as VIVOTEK's license plate recognition software, you can select to display different types of information. You can use the Edit display data to select or deselect the display elements.

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



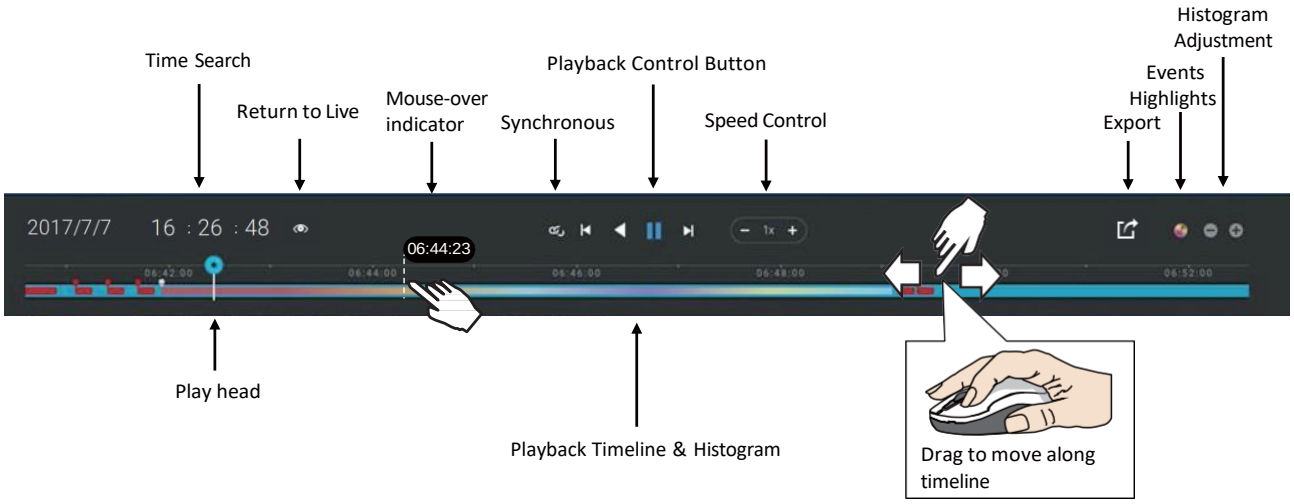
Below are the sample screens for applications implemented via the Data magnet.





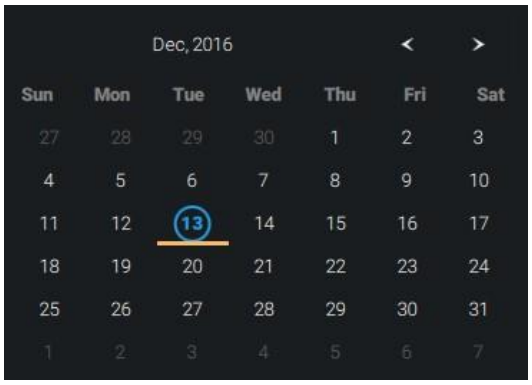
3. **Timeline Panel**: This panel appears when Playback is initiated.

The 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 follows:

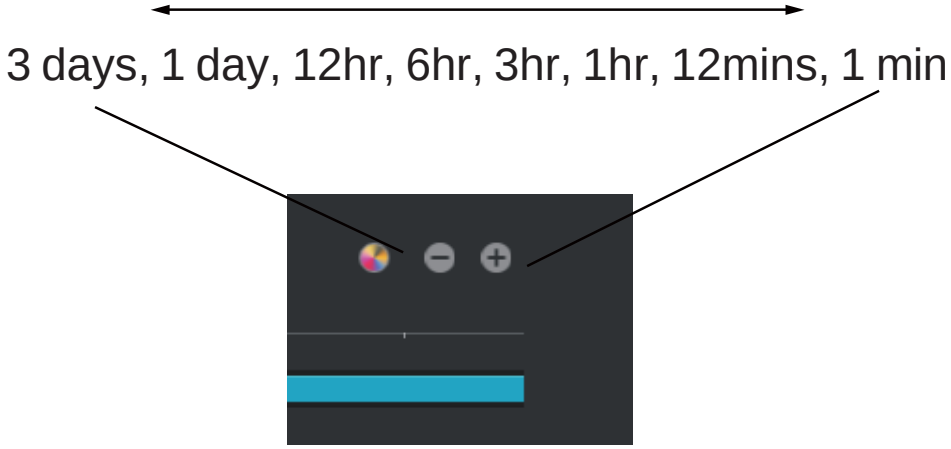
1. **Time Search**: Click on the current date to open a calendar. If you want to review videos recorded in another day, select it from the calendar.



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

Click on the current time. You can use the arrow buttons to change the time you wish to playback, or simply enter a preferred number. You can also pull the playhead along the timeline.

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

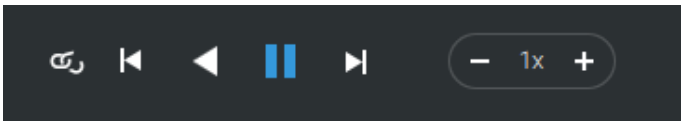


2. **Playback control**:

From left to right,

2-1. **Synchronous play**: This lets all cameras in the same view to playback video of the same point in time. If you perform synchronous playback on a multi-cell view, your computer can be stressed. It is recommended you create a new view with a 2x2 layout, select and insert camera views into it, and begin the Synchronous playback.

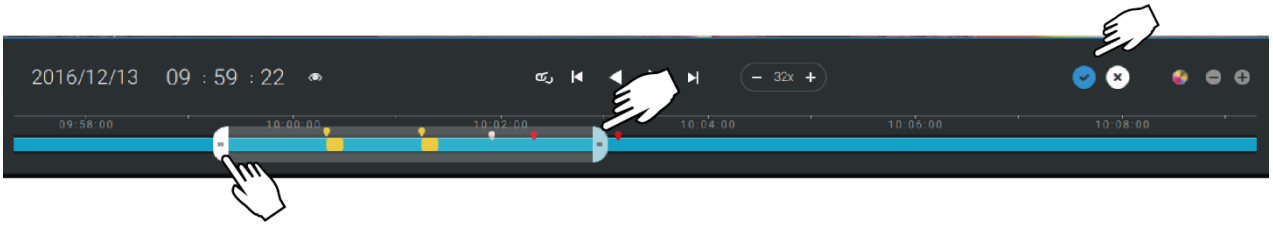
2-2. **Frame by frame buttons**: Click to move forward or backward to flick through the video frames. This may only display the I-frames.



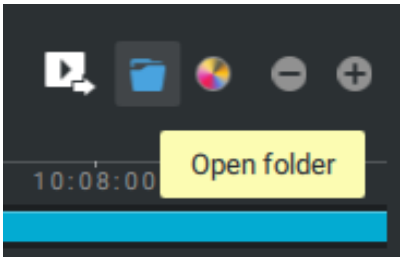
2-3. **Forward playback** and **reverse playback**: Click to view the video in the forward or reverse playback manner.

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

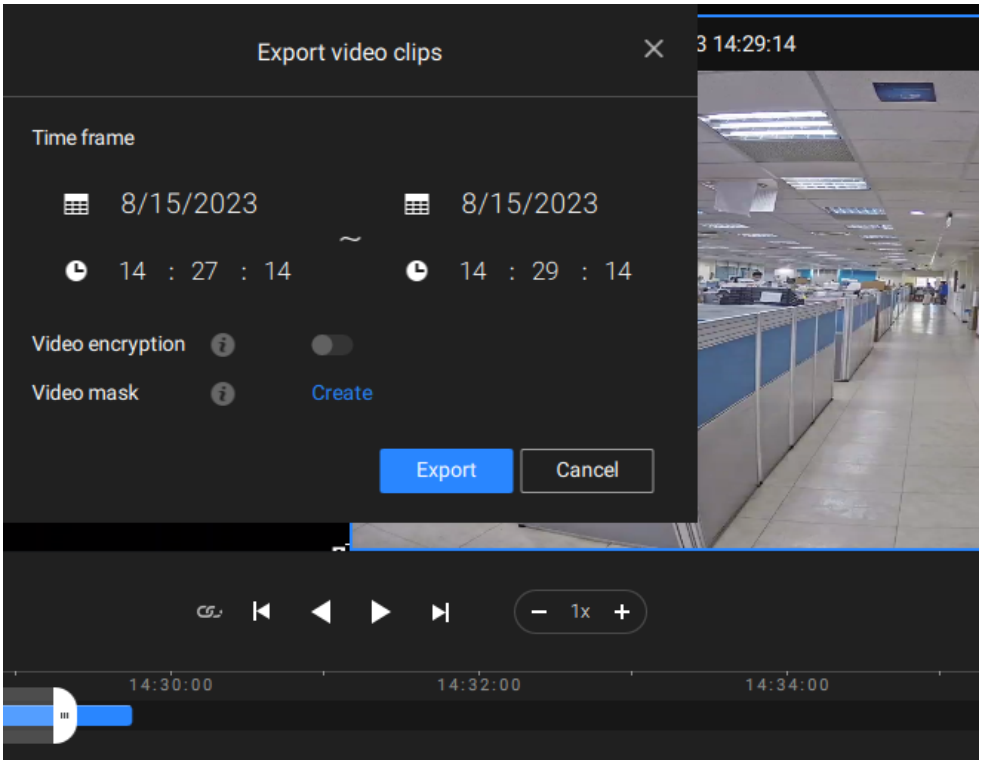
3. **Export Clips**: Click the Export Clips button . A range selector will appear. Pull the ends to include the time span you want to export. Note that each end of the selector, when clicked and selected, will turn white, and its location on the timescale is shown on the timeline. When done, click Start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

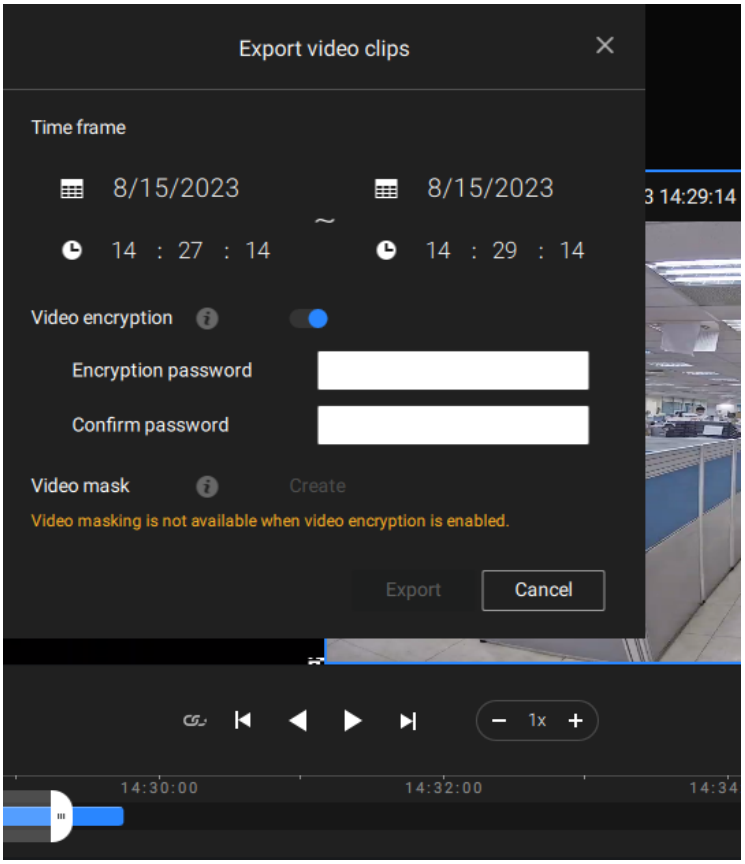


Depending on the length of video clips to export, it may take minutes to export. When the export is completed, a shortcut to the exported clips is shown. You may then open the folder where the clips are located.

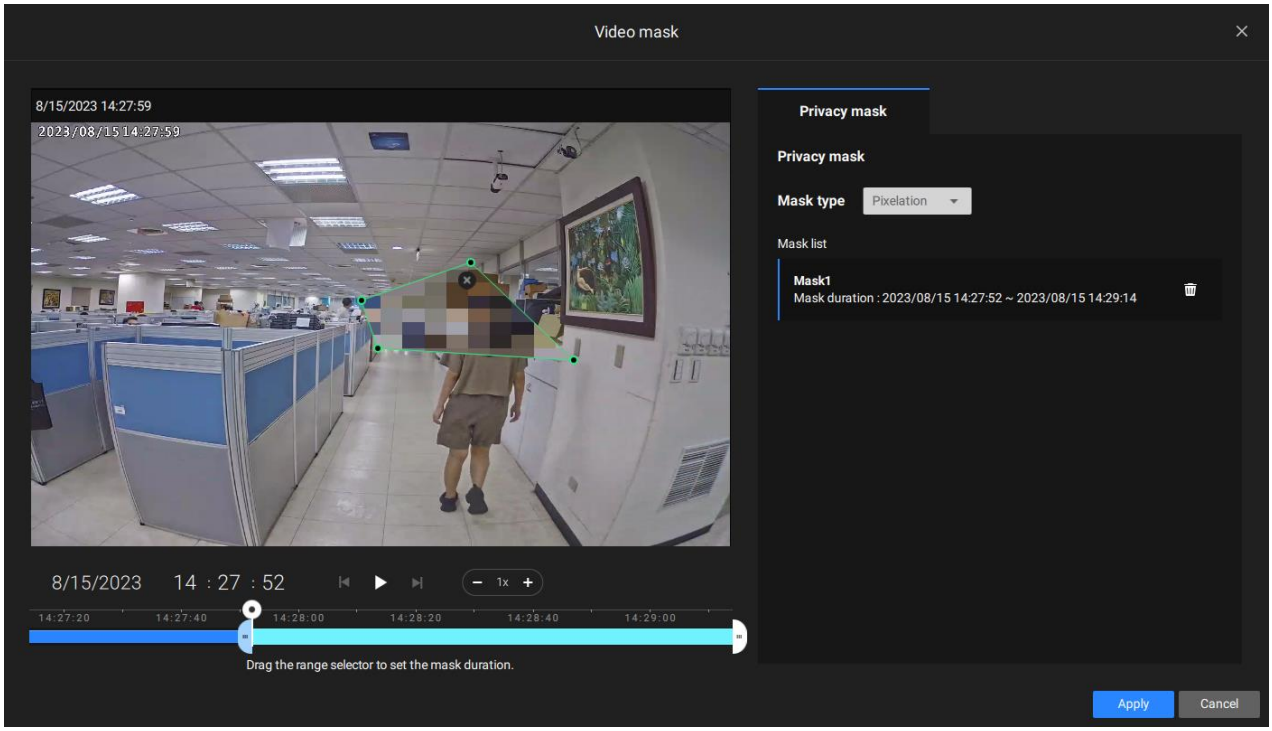


When you export a video, you can assign a password for the encrypted video. Once encrypted, you cannot play the video using ordinary video players. You can only play the video using VSS standalone player after you enter the correct password.





When video encryption is off (default), you can create video masks (available on VSS Professional only; black or pixelated) for specific time frames to protect privacy in the video to be exported.



NOTES:

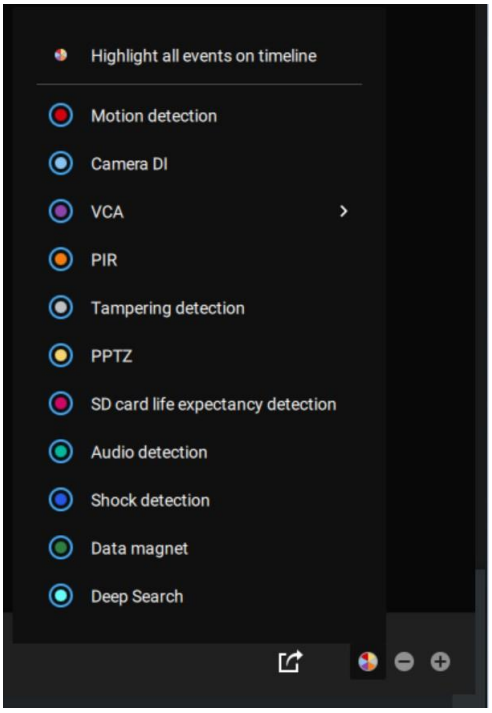
• A video mask overlays the original video and thus alters the raw data.

• Once a video with masks is exported, the video file format becomes 3GP H.264, and thus it is not necessary to use the VSS Standalone Player for playback.

• A video mask cannot coexist with any of the three functions: Video Encryption, Displayed Watermark over Video, or Digital Watermark.

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

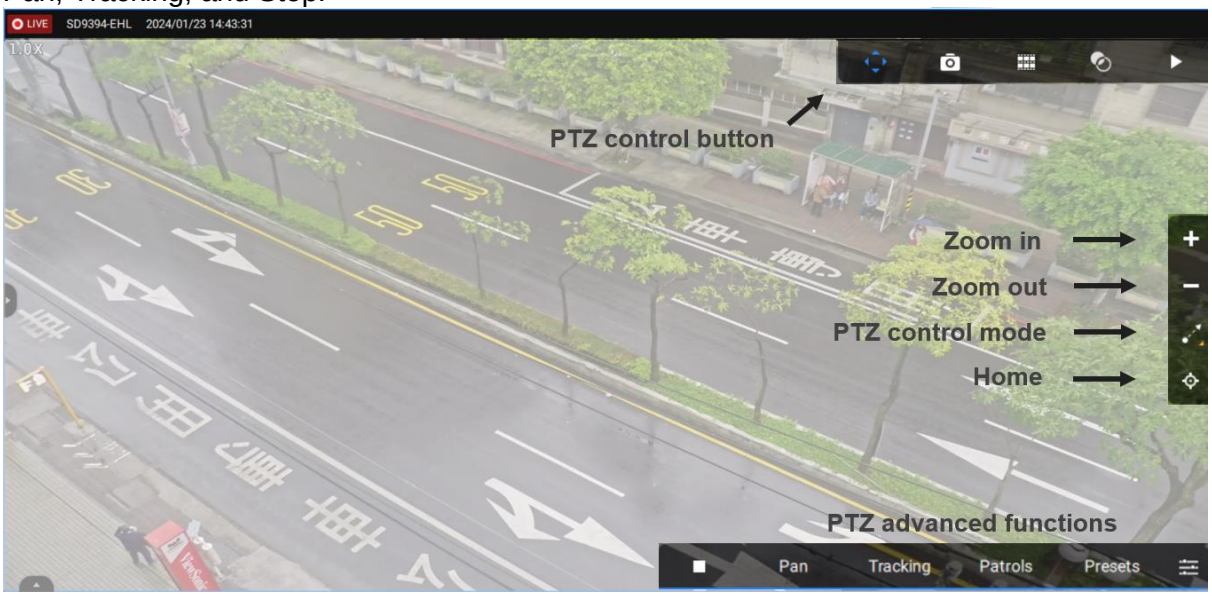
Note that on the VIVOTEK's Linux-based NVR, the timeline will display the occurrence of an event for a length of 10 seconds since its occurrence.



2-11. PTZ Control

PTZ control refers to the mechanical PTZ, which applies to cameras that are capable of pan and tilt directional control as well as zoom control.

To begin the PTZ control, click on the PTZ button .
A set of buttons will appear on the right side of the view cell, with functions arranged from top to bottom as Zoom in, Zoom out, Home, and PTZ control mode. Other advanced PTZ functions will appear in the bottom right corner of the view cell, including Focus, Zoom speed, Patrols, Presets, Pan, Tracking, and Stop.



Zoom in/out

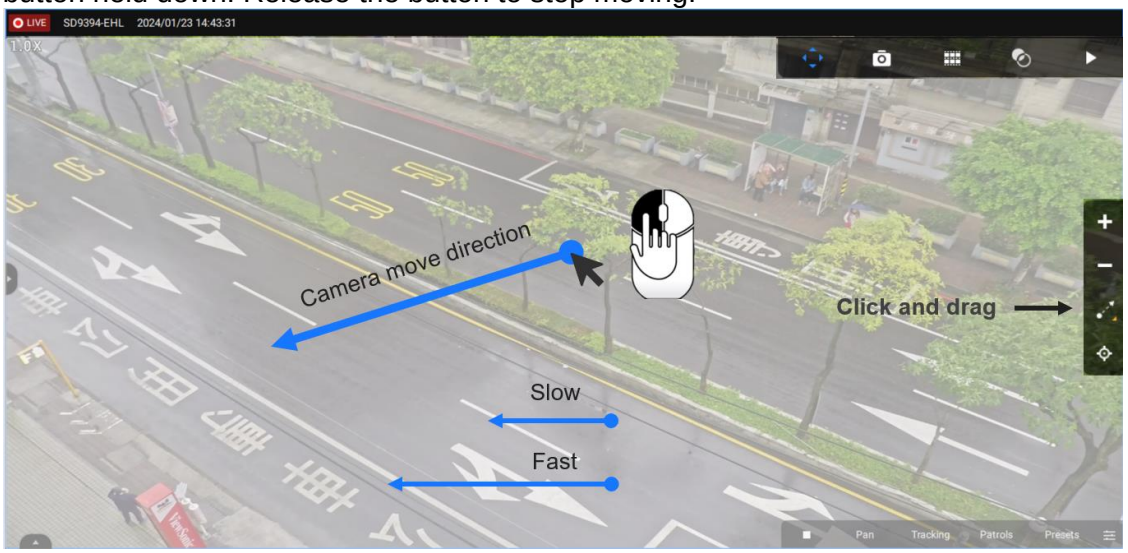
by clicking the zoom in + or zoom out − button, you can adjust the optical zoom of the camera; you can also use the mouse wheel on the view cell to zoom in or zoom out.

Home

by clicking the Home button , you can go back to the home position of the camera.

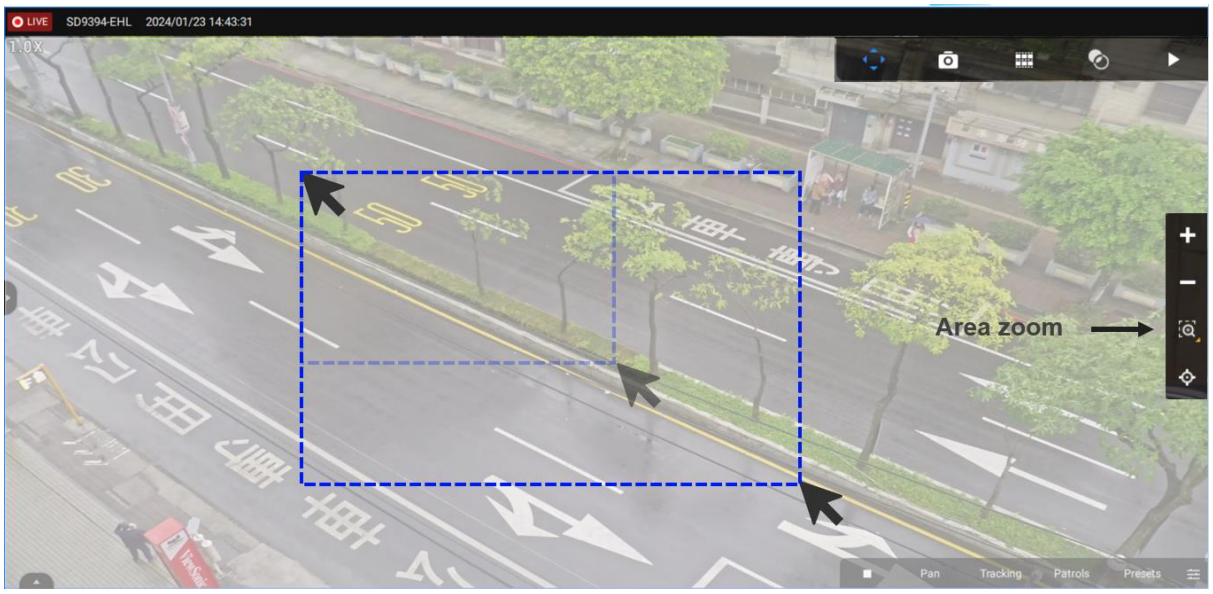
PTZ control mode

The default PTZ control mode is click and drag, which allows you to control pan and tilt by clicking and dragging your left mouse button across the view cell. A light blue trace will appear while you drag the mouse towards the direction you wish to move. The longer the trace, the faster the move. Note that while the camera is moving, you can change the move direction by keeping the mouse button held down. Release the button to stop moving.

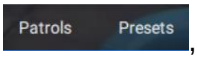


You can also click the PTZ control mode button to switch to the area zoom mode, which allows you to draw an area on the view cell for zoom in.

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



Advanced PTZ functions

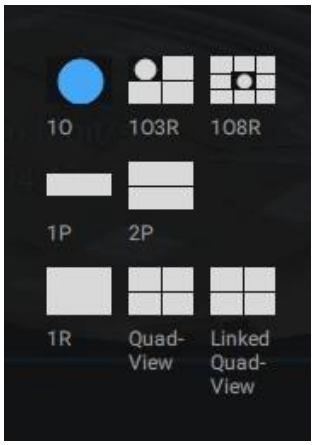
By clicking the patrol and presets button 

, there will be a dropdown list that allows you to select the patrol or preset. By clicking the stop button  , you can stop the movement or action of the camera.

By clicking the tracking button, for cameras that support smart tracking advanced, there will be a preset list that allows you to select which preset you want to enable tracking. For other cameras that support smart tracking or auto tracking, the camera will start tracking with the current position. You can also adjust the zoom speed, focus, and focus speed manually or start pan by using the button  .

2-12. Fisheye Camera Dewarp Modes

By default, a circular view is displayed when a fisheye camera is successfully connected.
To display Regional, Panoramic, or a 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.

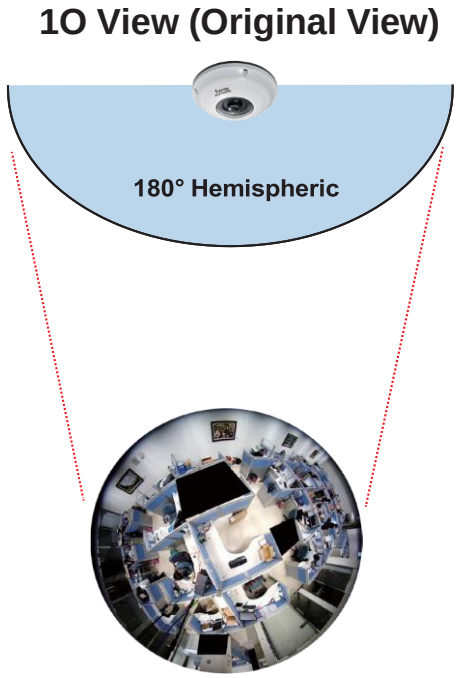


The display modes available are: 1O (Original), 1P (Panoramic), 1R (Regional), 2P (2 Panoramic), 1O3R (1 Original & 3 Regional), 4R (Quad Regional), 1O8R (1 Original & 8 Regional), and 4R Pro (4 Proactive) modes.

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

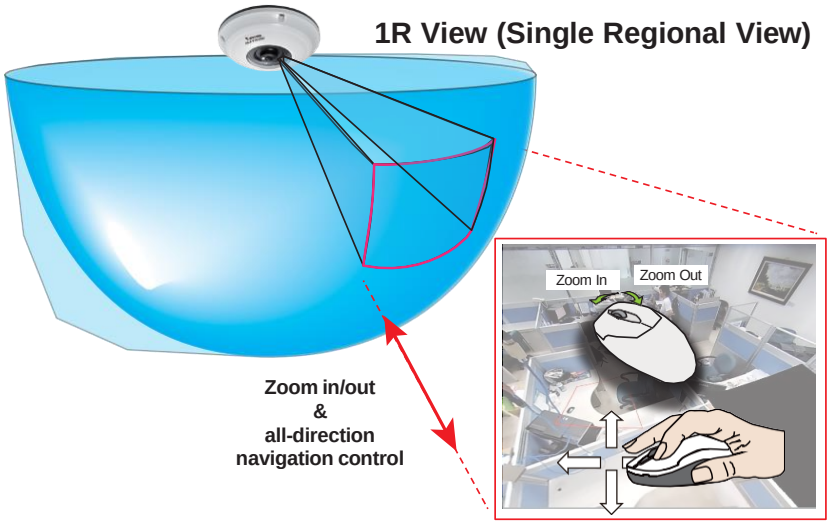
1O (Single Original) Display mode:

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



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.



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:

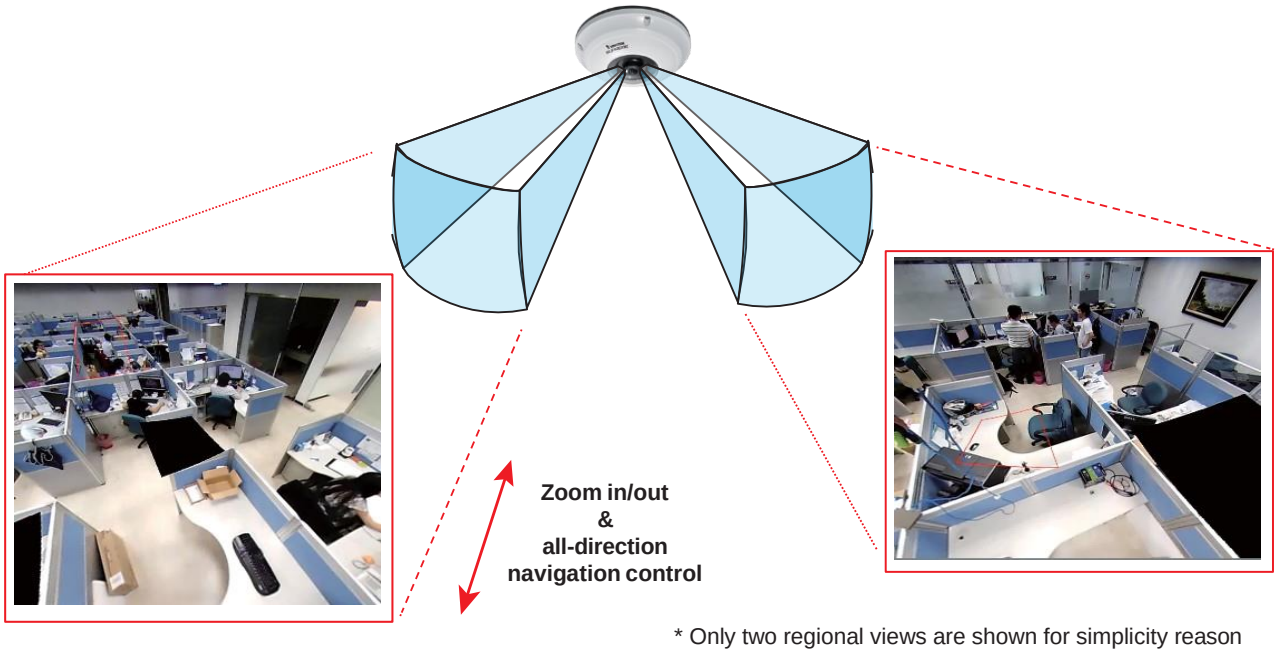
Two dewarped rectangular views are placed one on top of another each showing 180 degree of panoramic view. The 2P view looks like the upper view shows the front of hemisphere, and the lower view the rear half of the hemisphere.

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.

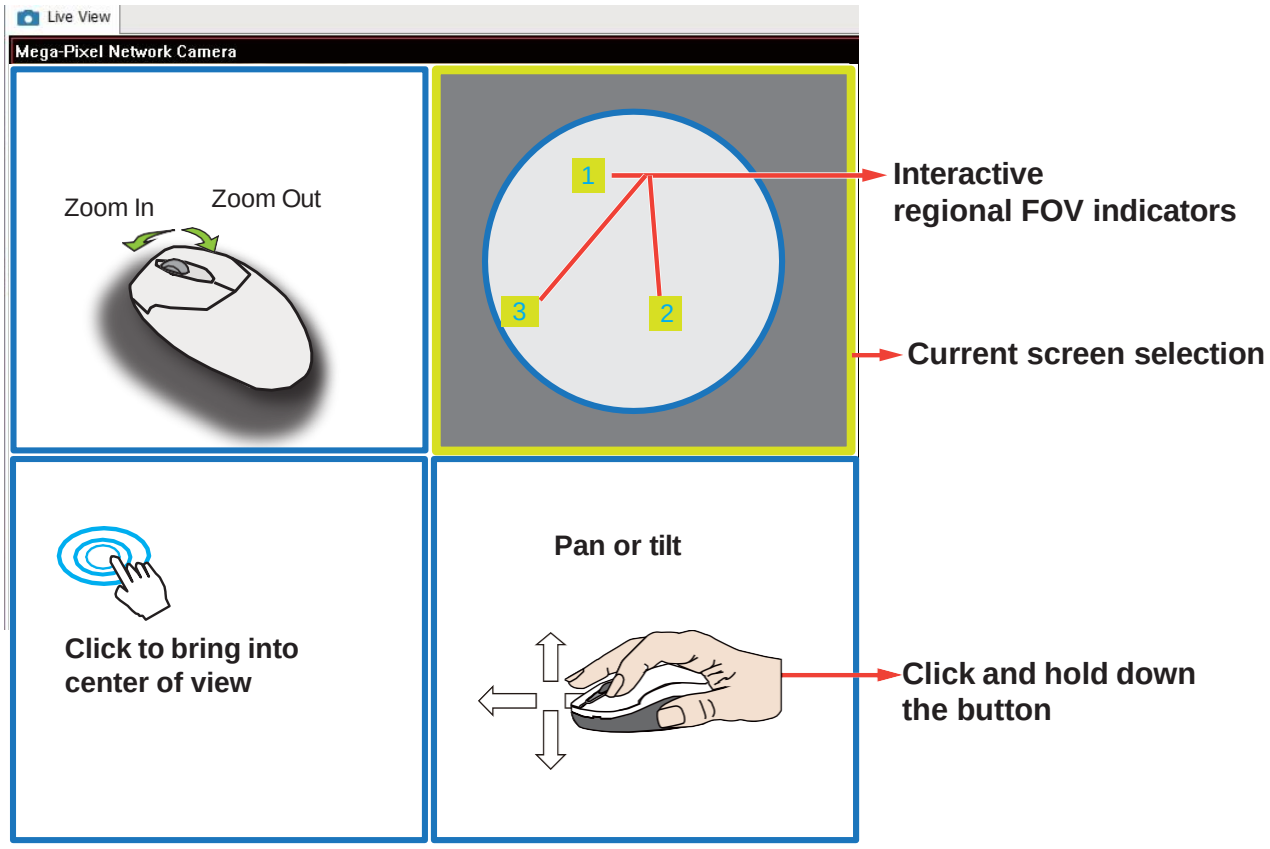
PTZ Mouse Control

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



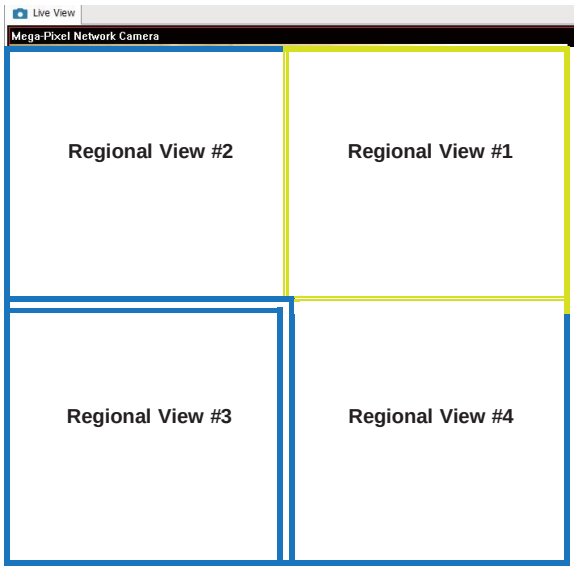
Below are the conceptual drawings for the other display modes. The available display modes can differ with different mount types:

Regular: 1O, 1P, 1R, 1O3R, 4R.

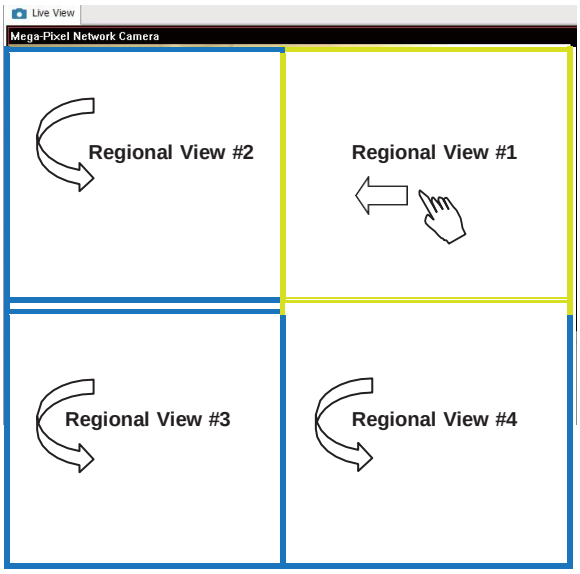
Wall mount: 1P2R, 1P3R.

For more information, you can refer to fisheye camera's user documents.

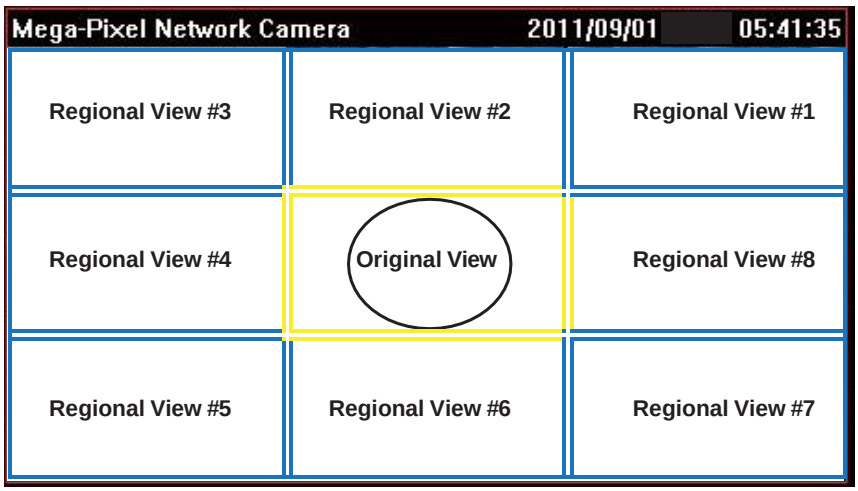
4R (Quad Regional) Display mode:



4RPro (4 Regional Proactive) Display mode:



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



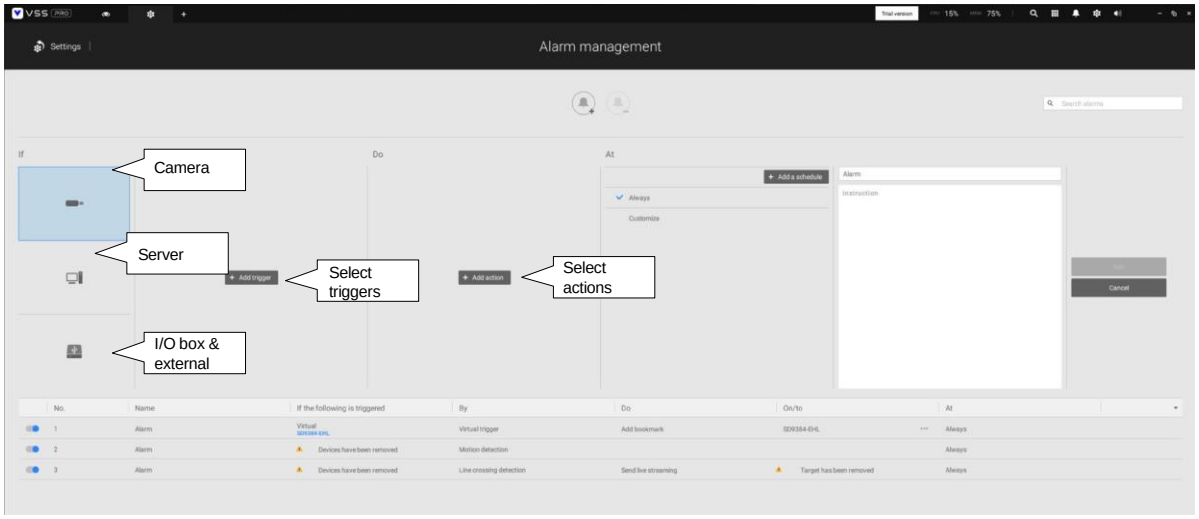
3rd-party Fisheye Dewarp

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 circle with the fisheye's circular view.

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

2-13. 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 VSS server can start a recording or send an Email notification when Motion detection is triggered.

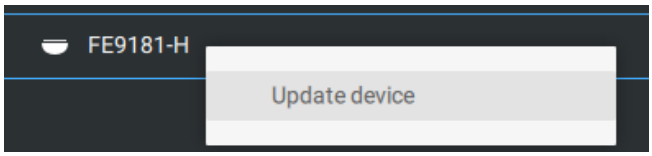


A wide variety of triggering conditions can be applied, including:

1. Camera triggers 

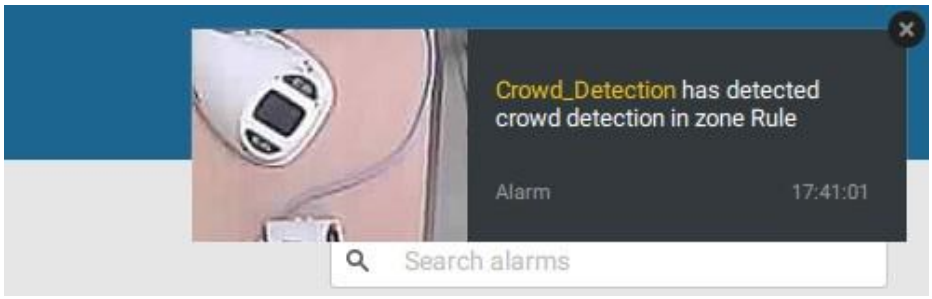
General			
●	Motion detection	●	IR (Infrared)
●	Camera DI	●	PIR (Passive Infrared)
●	Camera DO	●	Tampering detection
●	Temperature	●	Stop recording
●	Recording error	●	Audio detection
●	Video loss (Video server only)	●	Shock detection
●	SD card life expectancy detection		
Video Content Analysis			
●	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 VSS device tree, right-click on the device to perform a manual refresh "Update device" to acquire the latest configuration update.

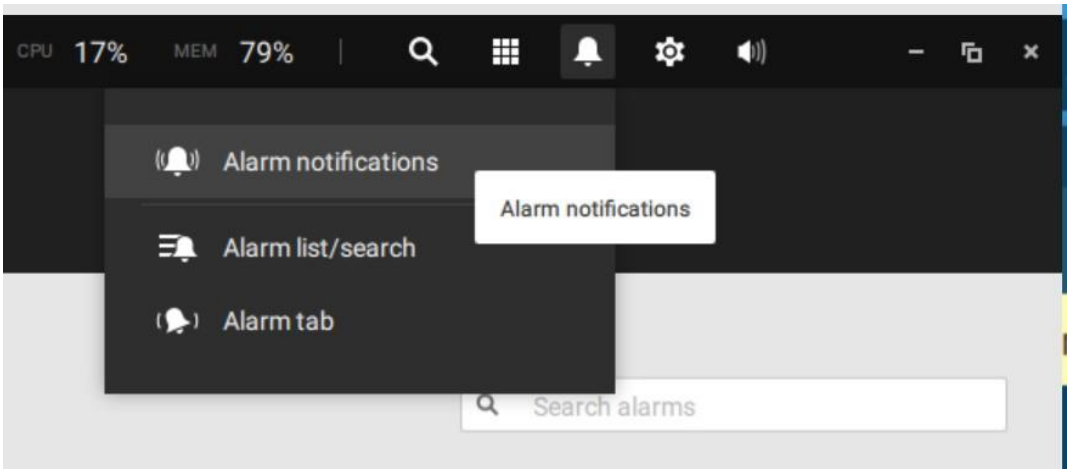
If a triggering condition is associated with event recording, an event prompt will pop up on the screen when a triggering condition is met. For example, the number of people exceeds a preset threshold in a Crowd Detection configuration. The sample prompt is shown below. The related footage can be played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



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.

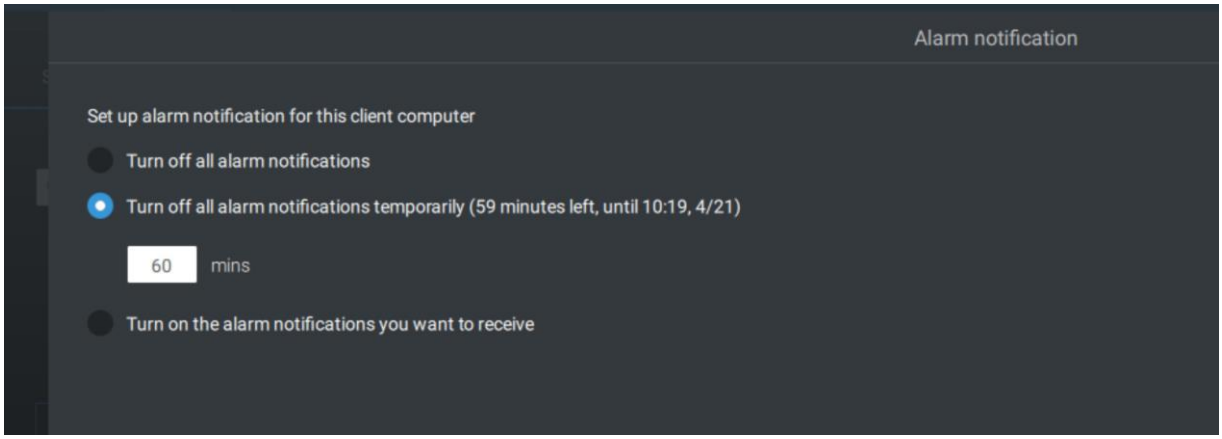
The notification configuration is kept on the client computer.

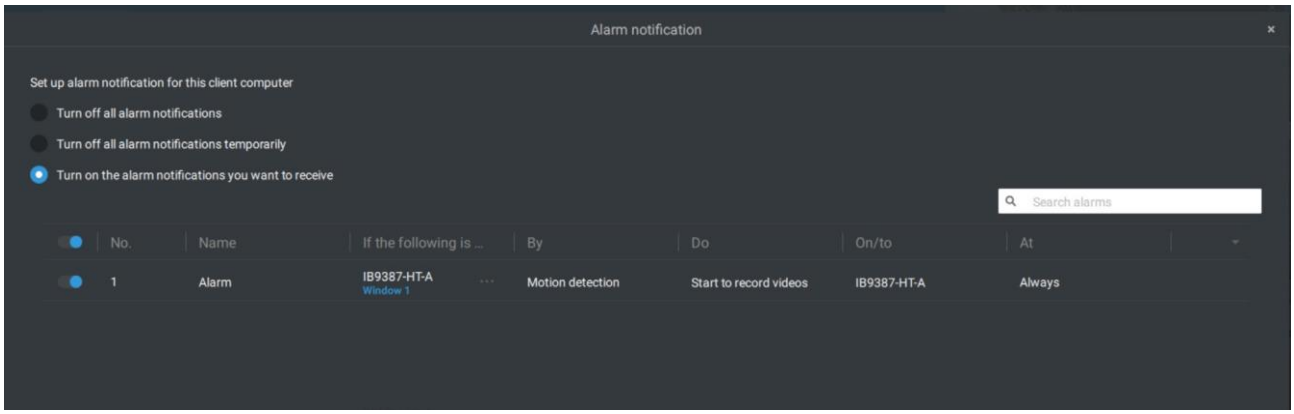
When the Alarm notification is turned off, the Alarm tab icon is greyed out .



Individual VSS 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.



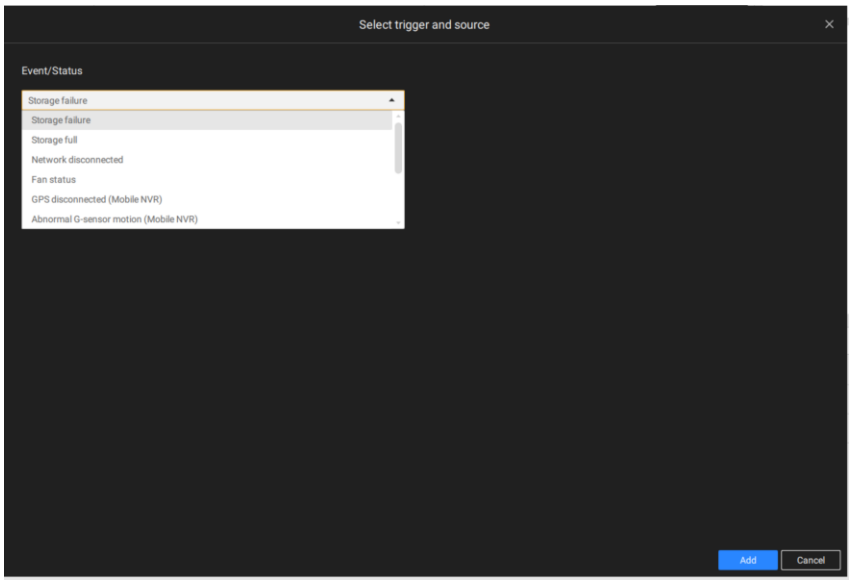


Note that the default for the alarm notification is "Turn on the alarm notification you want to receive." If you turn off the alarm notification, you need to re-activate it after you turn off the notification the first time.

2. 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.



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."

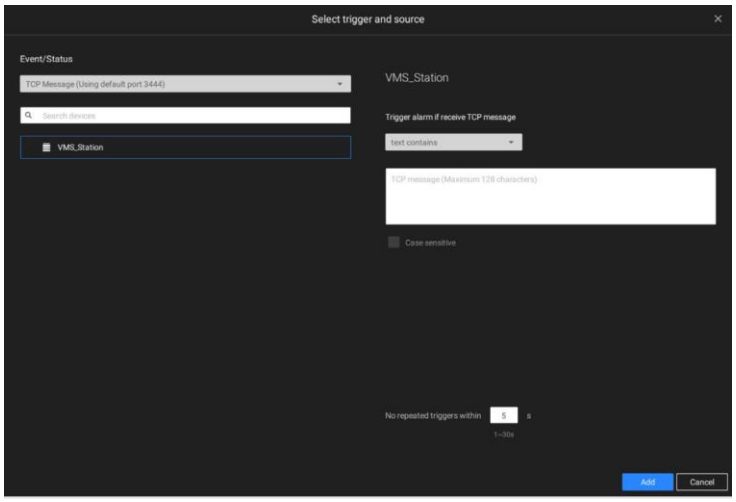
For I/O box configuration, please refer to the I/O Box page.

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 VSS servers or external sources (such as an access control system) via the analysis of received TCP messages 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 a bookmark, play an audio file, send HTTP requests, etc.

To configure a TCP message trigger,

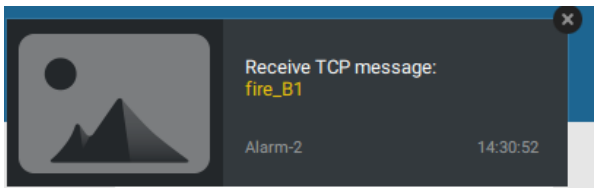
Select TCP message as a trigger type, and enter a description, such as a short term, for VSS to listen and analyze data packages.



Below are the messaging parameters:

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



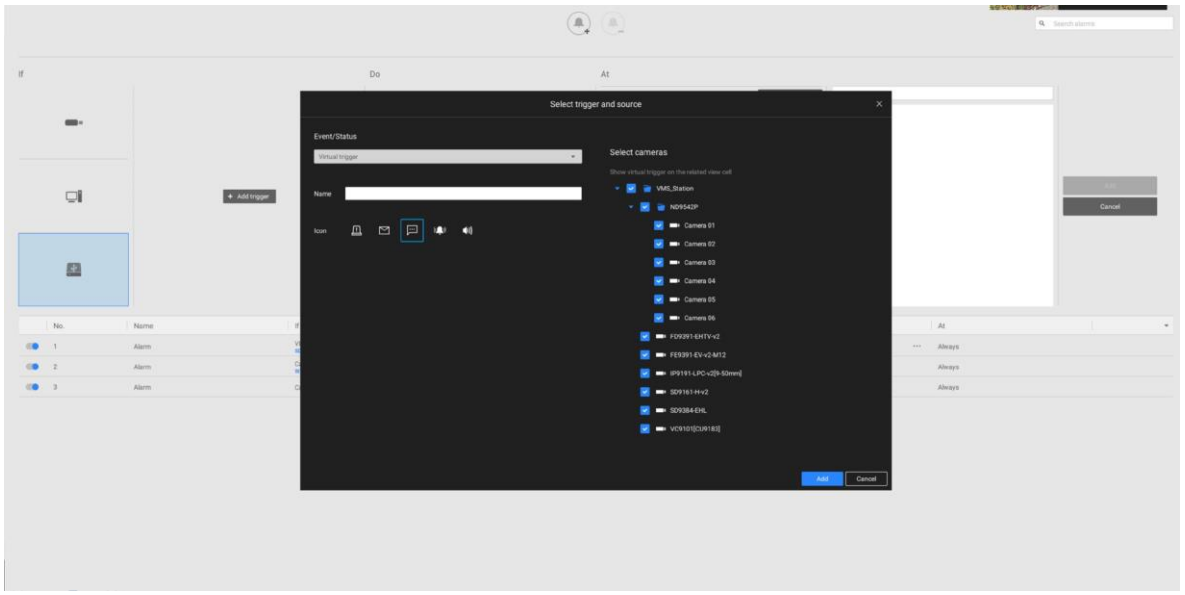
Virtual triggers have the following benefits:
1. More operation control, e.g., got to camera preset, add a bookmark, play an audio file with network audio devices.
2. Integrating 3rd-party systems and devices; using the Send HTTP requests; setting DO status commands.

To configure a Virtual trigger,

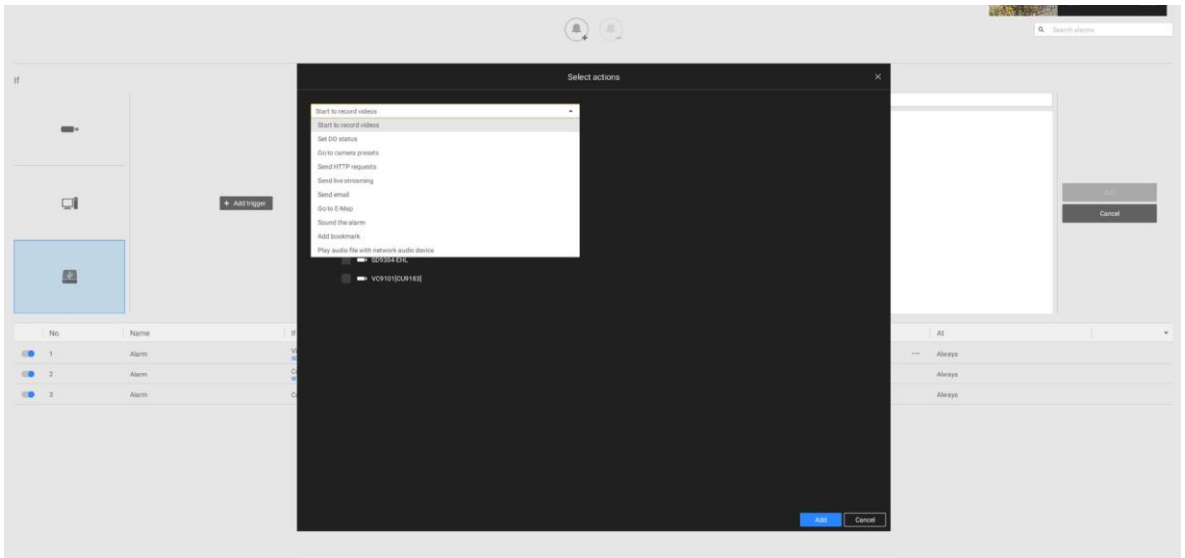
Go to Settings > Alarm > Add alarm.

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

The Select trigger and source window will prompt.

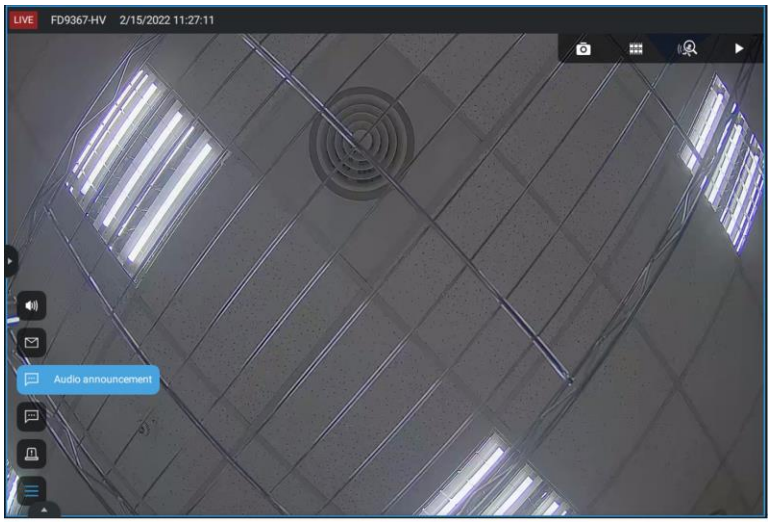


Select the alarm action.



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

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



Select the External device event, and then click on the Add action button.
The Select actions will prompt.

The available actions include:

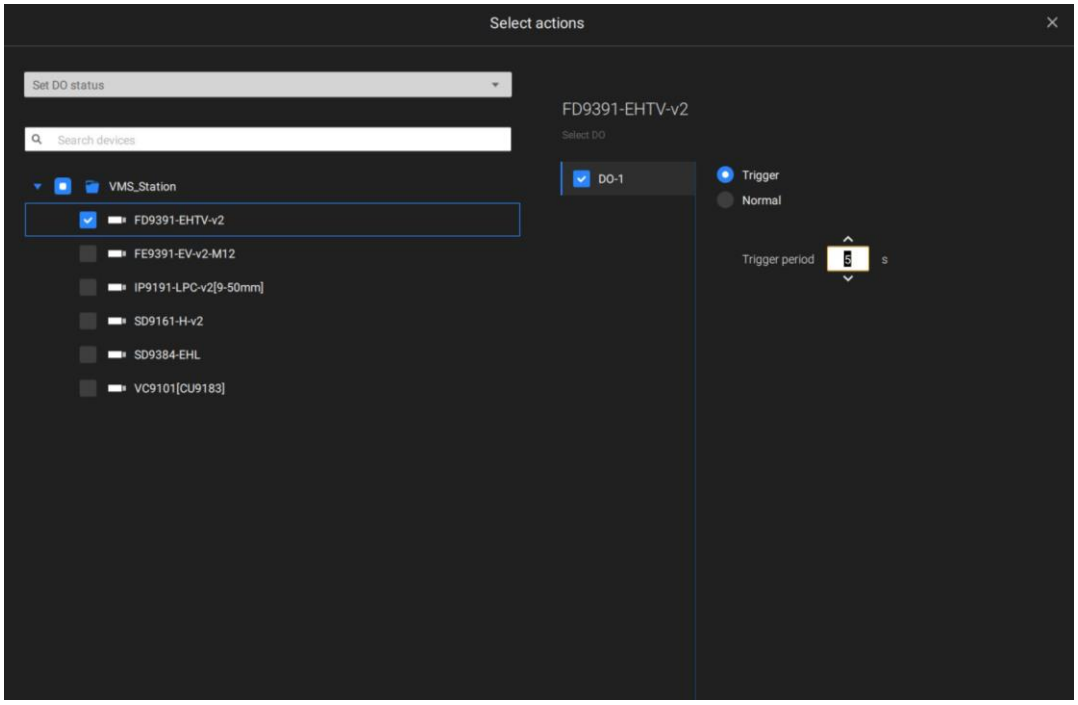
●	Start to record video	●	Send HTTP requests
●	Set DO status	●	Send live streaming
●	Go to camera presets	●	Send email
●	Go to E-map	●	Sound the alarm
●	Add bookmark	●	Play audio file with network audio device
●	Send mobile notification		

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.

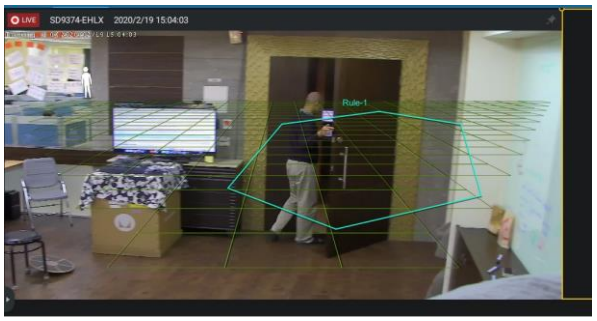
Set DO status will activate a DO connection. For example, to light an illuminator or sound an alarm.

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.



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



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.

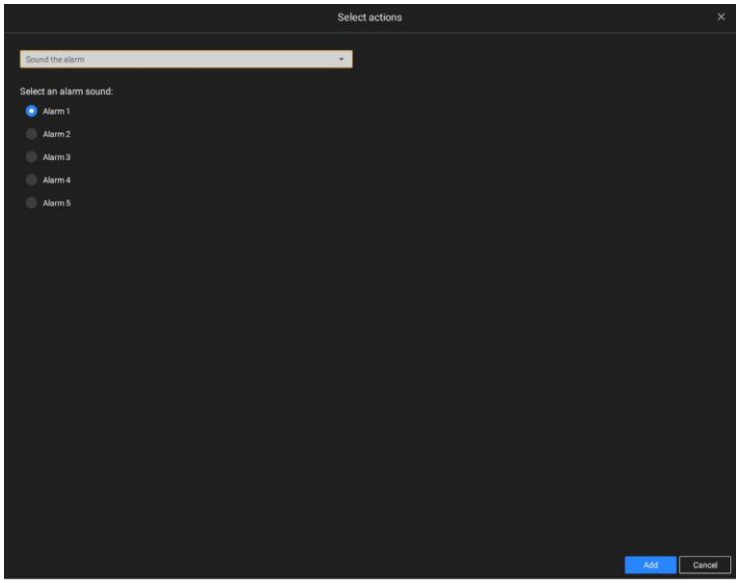
The VSS server automatically disables unavailable options. For example, when the DO option is selected, the cameras that do not support DO connections will be hidden.

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.

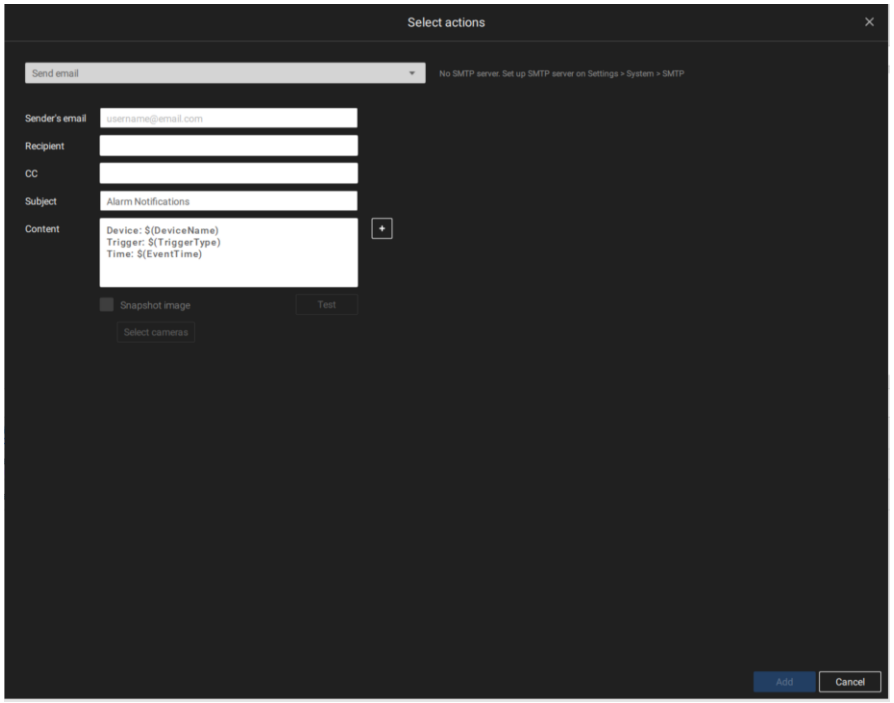
Go to E-map opens a pre-configured E-map of where the triggering condition occurs. The user can then click on the camera icon on the E-map for an instant viewing.

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.

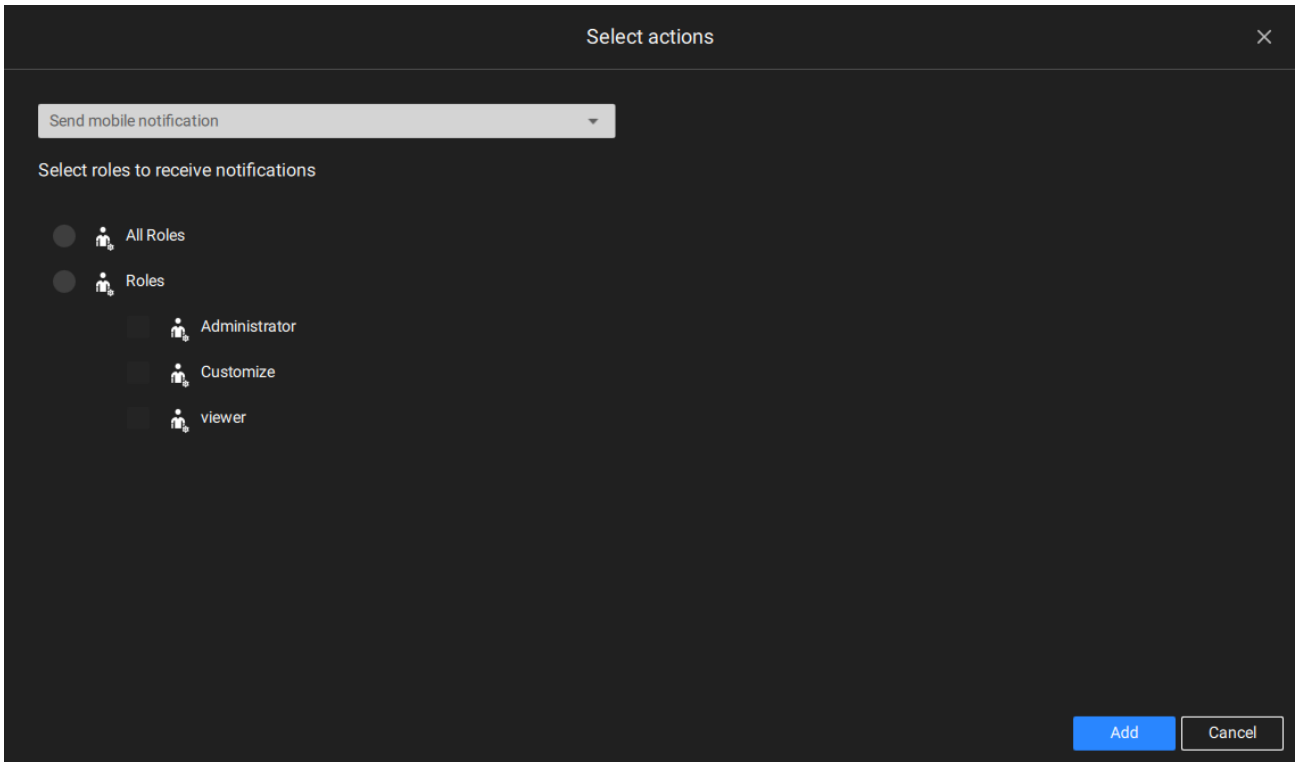
Sound the alarm action provides 5 alarm sounds that will be sounded on the VSS client or server. Your VSS client or server should have speakers for playing the audible alarm.

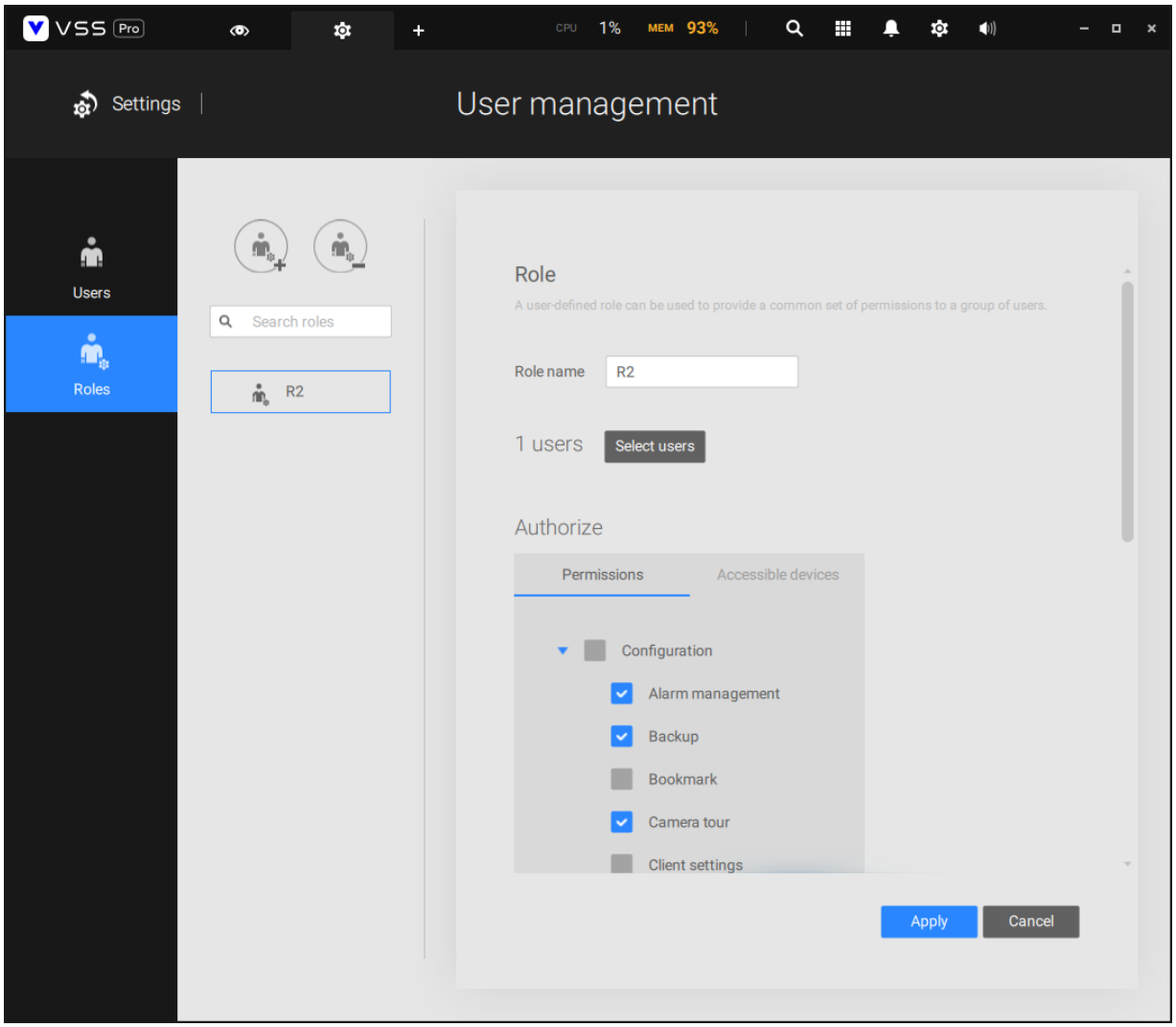


A reachable Mail server and Email accounts must be provided before you can apply the settings.

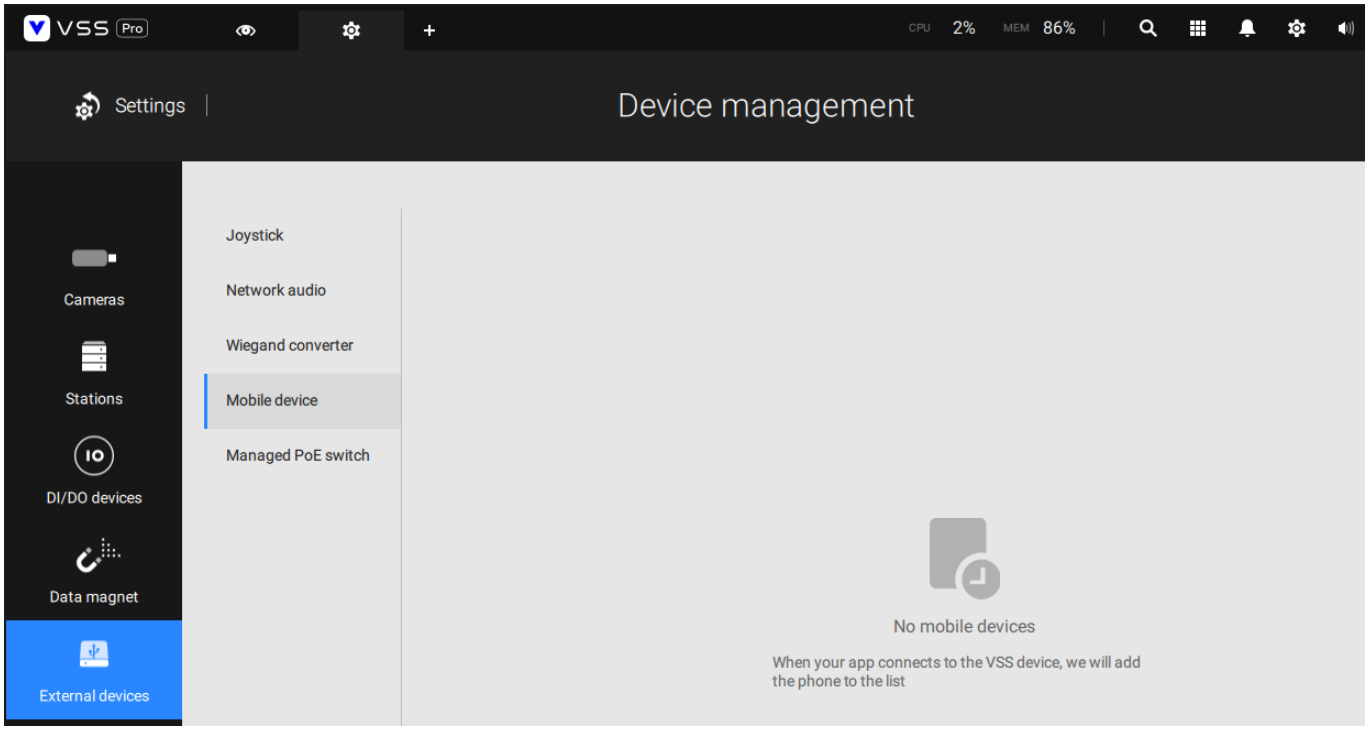


Send mobile notification, by default, pushes instant alarm contents to the iViewer mobile app on the smartphones of users. Meanwhile, the User-defined roles option is available (only on VSS Pro) for choosing a set of roles and saving the set as a role profile. So, it is easier to assign a user to a user-defined role.



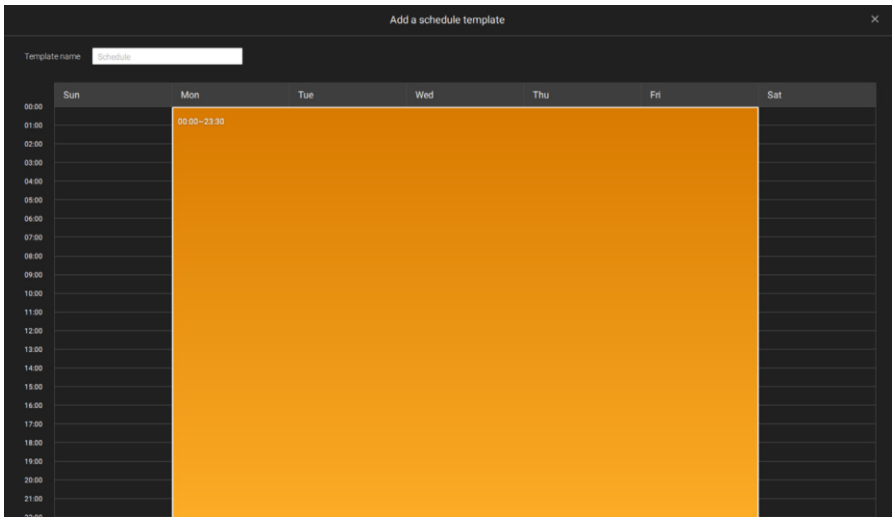


In addition, the administrator can click Settings > Device > External devices > Mobile device to query which mobile devices are using iViewer to log in VSS and to turn on (default) or turn off sending the push notification to a user's mobile device (phone).



In other words, every user joining the VSS server can receive push alarm notifications by default. Once you remove a user from the notification list here, if this user logs in to VSS again, the user can still get alarm notifications. Therefore, if you must remove the user from the notification list permanently, change the user's password or delete the user account directly.

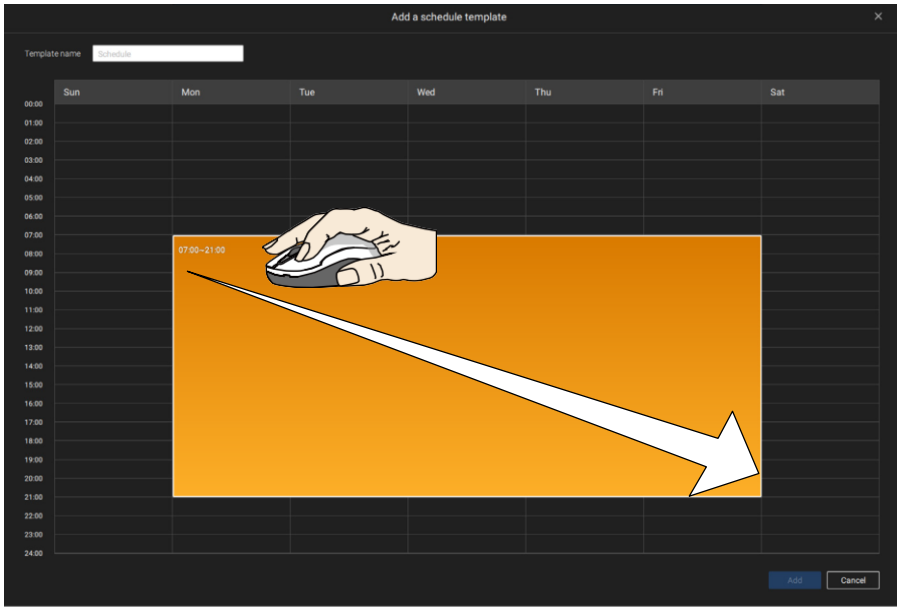
On the **Schedule** page, you can select to activate or de-activate alarm triggers throughout a specific timeline. For example, in some situations you can disable the alarm triggers during the office hours, and choose to enable the triggers only during the off-office hours.



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

You can manually create a effective time template using the New template

button.



Click and hold down on the time cells, and drag the mouse to include the time span of your preference. 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 configuration window applies to both the Schedule template and the customize schedule windows.

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

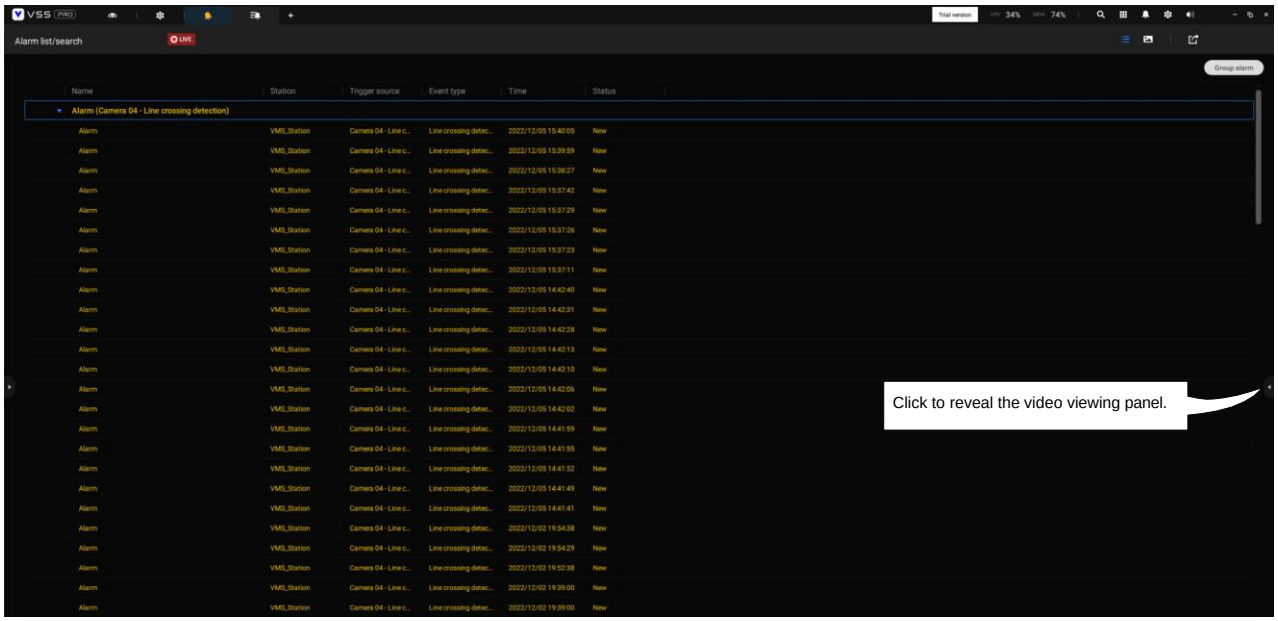
Enter a name and instructions for users to follow, and then click Add to complete the Alarm setting.

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

Group Alarm

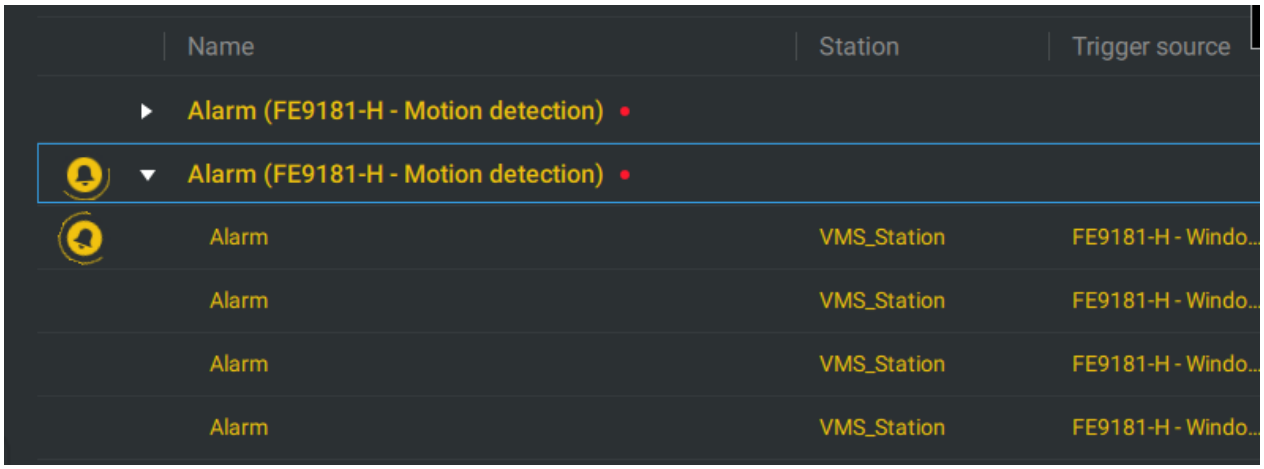
Multiple triggered alarms can be presented as group alarms. Alarms triggered by the same event type, and by the same camera can be grouped together. In this way, multiple similar alarms can be listed under one entry.

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

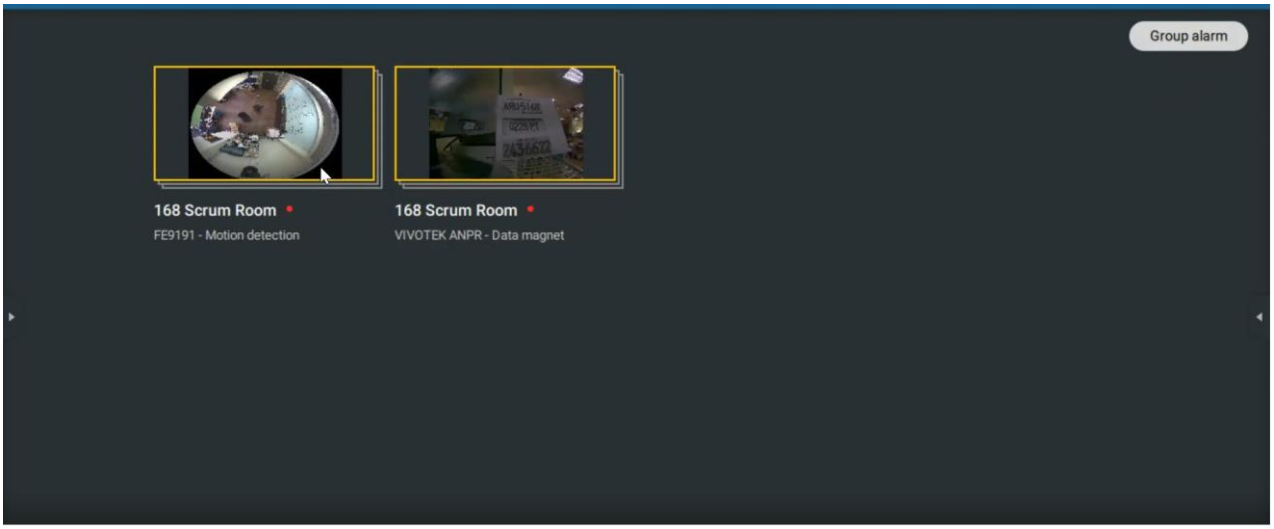


In the list mode, you can expand the right-hand-side panel. The video of the latest alarm will display.

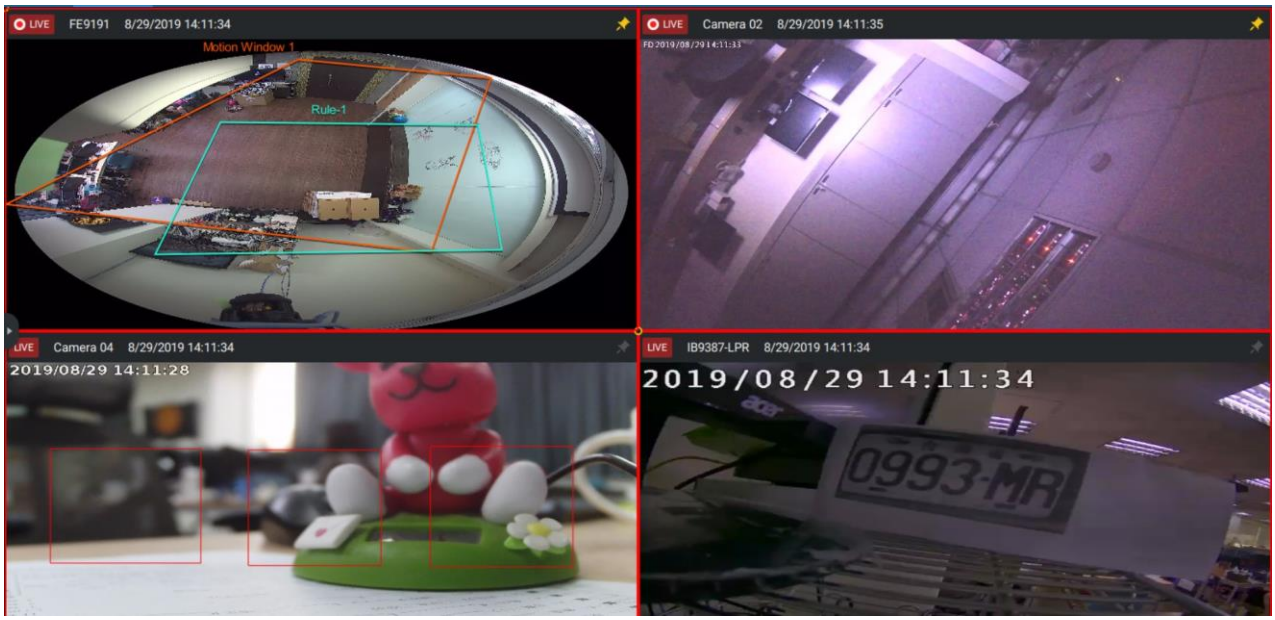
When the alarm-triggered action is configured as a sounded alarm, you can mute all alarms in the group by clicking the alarm sound icon.



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



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



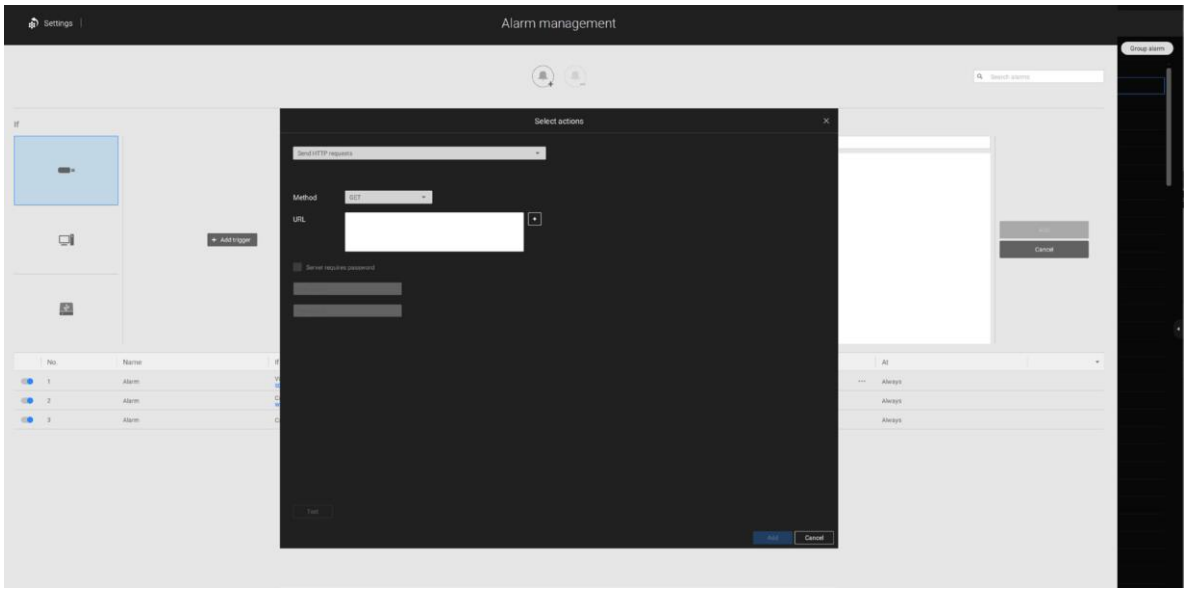
In the Alarm tab window, use the thumbtack  button to freeze the current screen. If thumbtacked, the other incoming alarms will not affect the current screen.

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

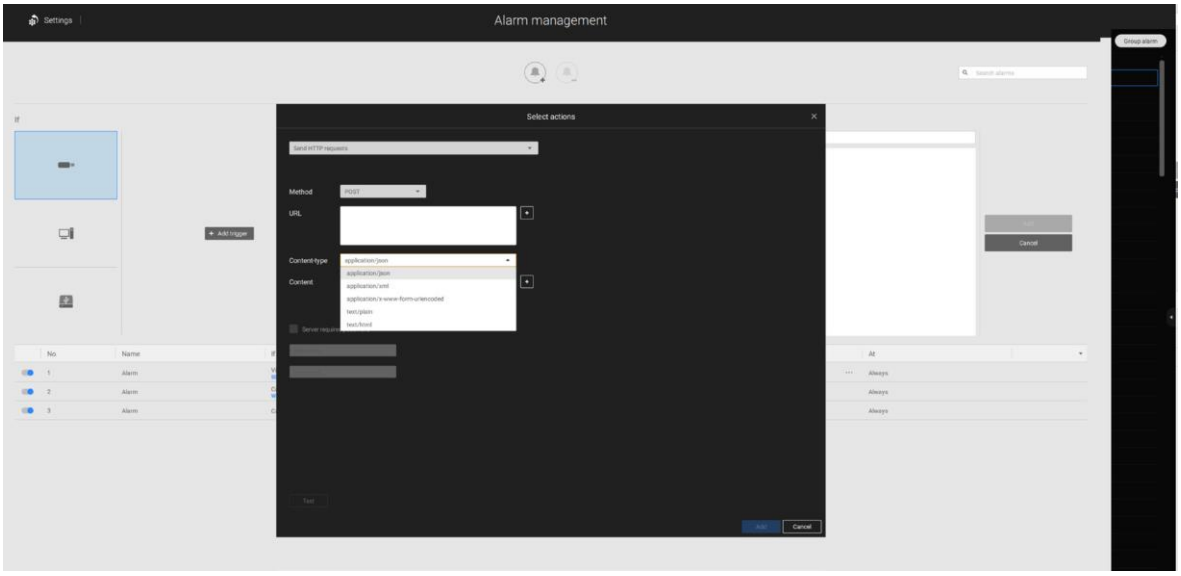
Configuring Send HTTP requests

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.

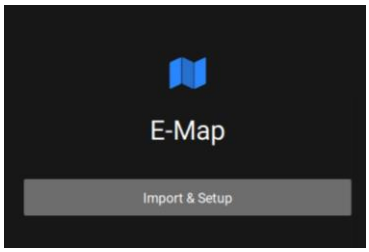


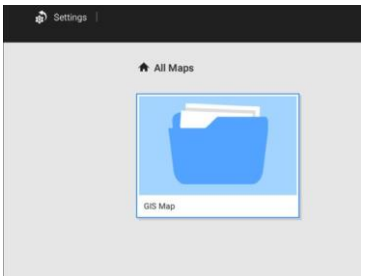
Below is a screen for setting the POST command. Enter the target resource's URL address, the content, and select the content type. If the need should arise for more content types, you can contact VIVOTEK's technical support.



2-14. E-Map

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

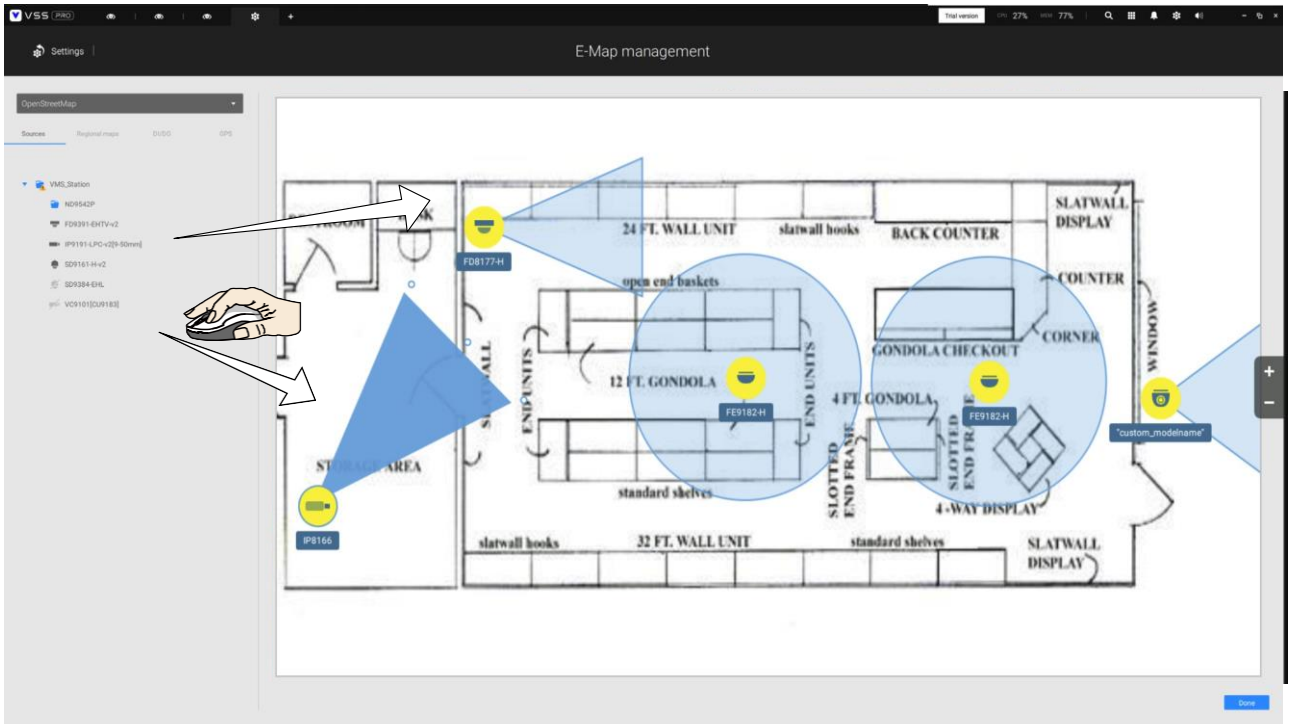




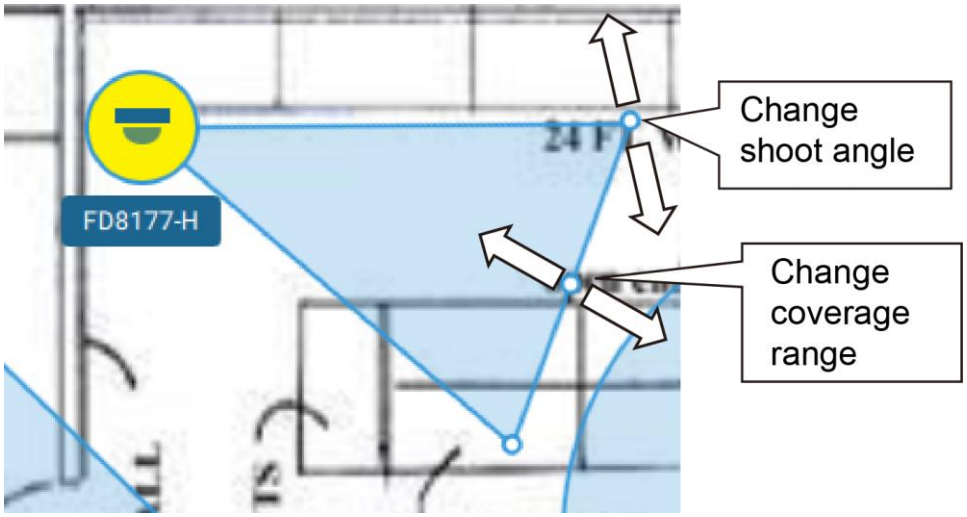
Click Import file or Import folder . An entire folder can be imported.

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

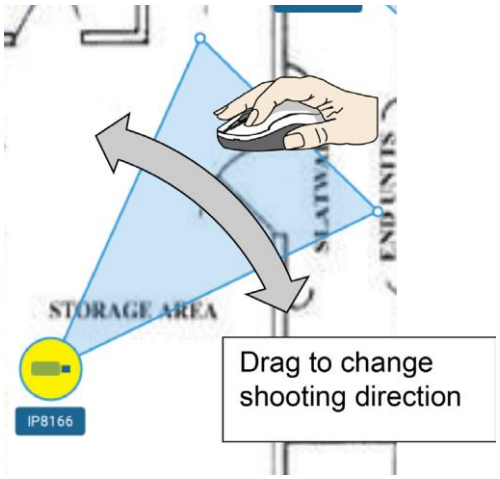
Your cameras will be listed on the left. Drag and drop the cameras to the corresponding locations on the map.



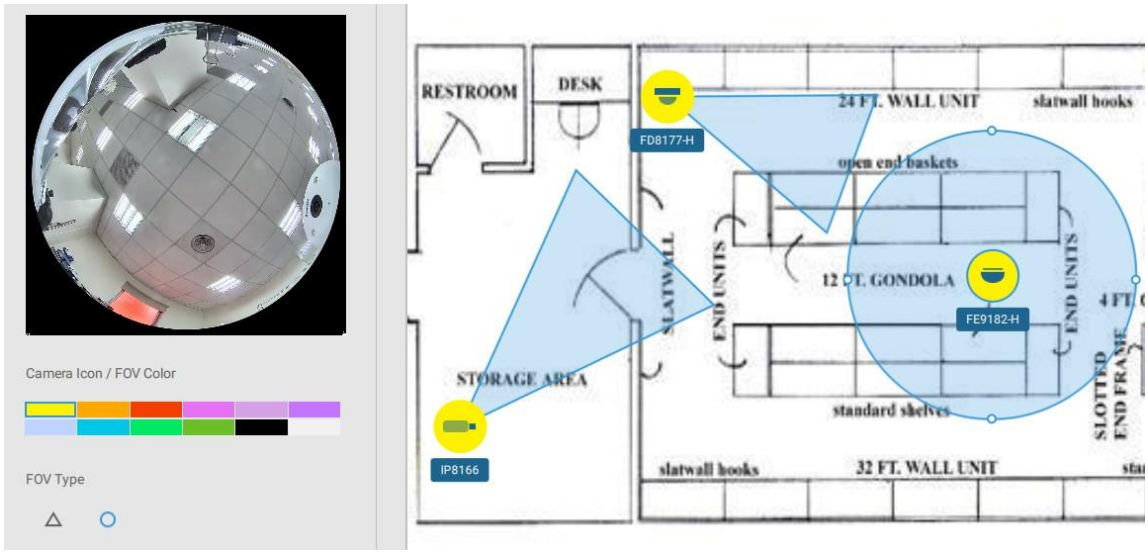
When the camera is in place, drag the FOV indicators on the edge to change the shooting angle and the coverage range.



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



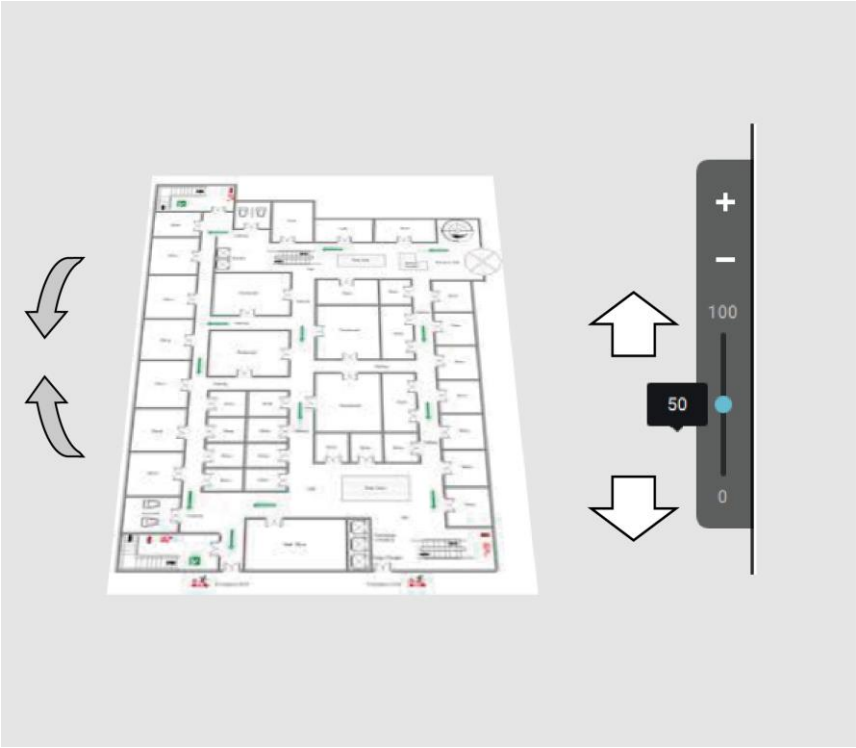
Click on the camera icon. You can also change the color of camera icon and the FOV type. Fisheye cameras, when ceiling mounted, have a round shape coverage.



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.



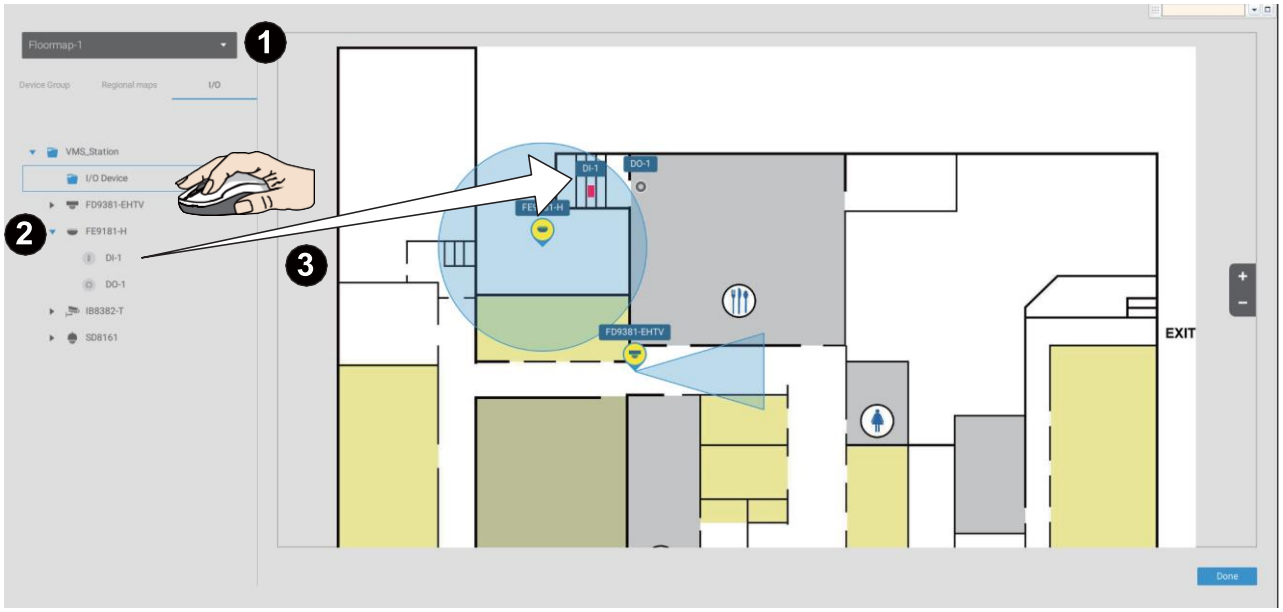
Placing DI/DO Devices

I/O devices can also be planted into an E-map, such as alarms 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.

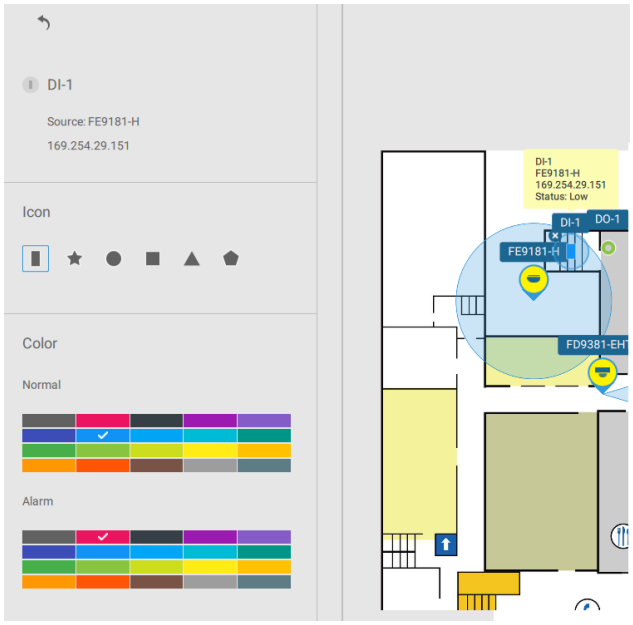
2. Unfold the sub-trees beneath the network camera, (taking camera DI/DO devices as an example).

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



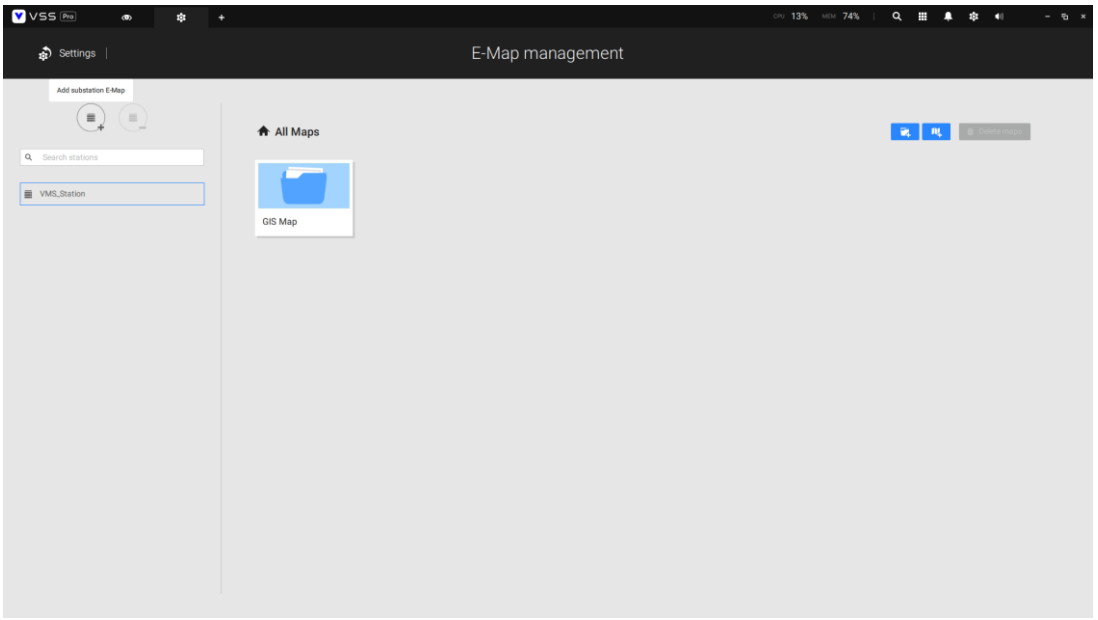
Uploading Substation E-map to CMS

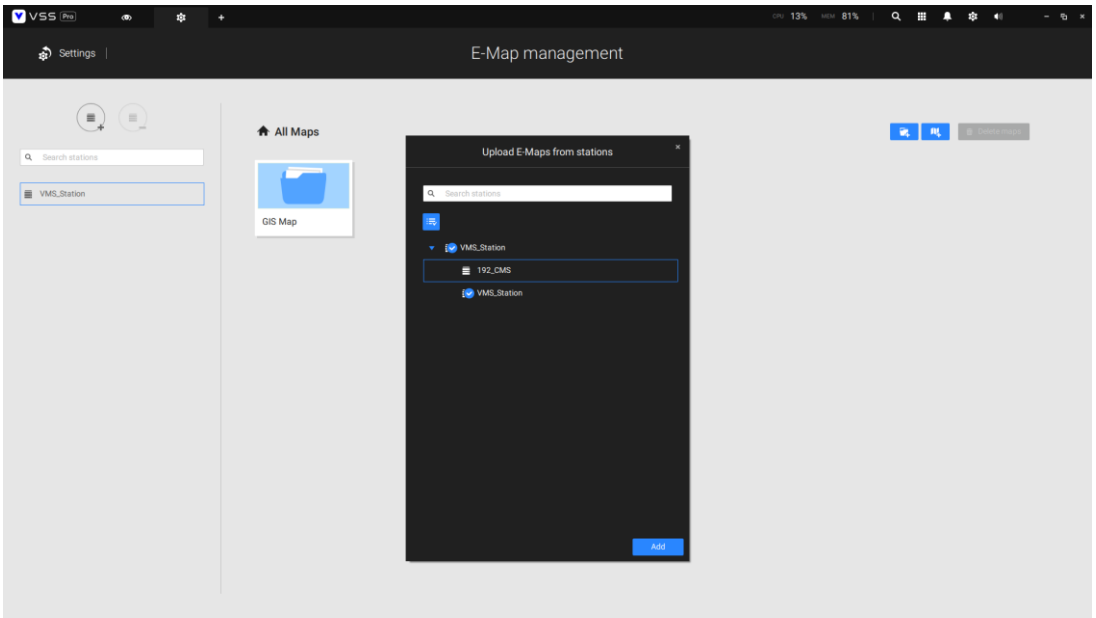
This feature allows users to manually transfer E-Maps created on substations to CMS, saving time on redundant E-Map creation. Here are the operational steps:

1. Navigate to Settings -> E-Map.
2. Select "Add Substation E-Map."
3. Choose the specific substation E-Map you want to upload.
4. Once uploaded, the Substation E-Map becomes accessible in the E-Map function.

Notes:

1. Uploaded substation E-Maps do not automatically sync. If there are updates in the substation E-Map, a re-upload is required from CMS.
2. Editing the content of substation E-Maps is not allowed on CMS. Updates must be made on the substation itself, followed by a re-upload to CMS.



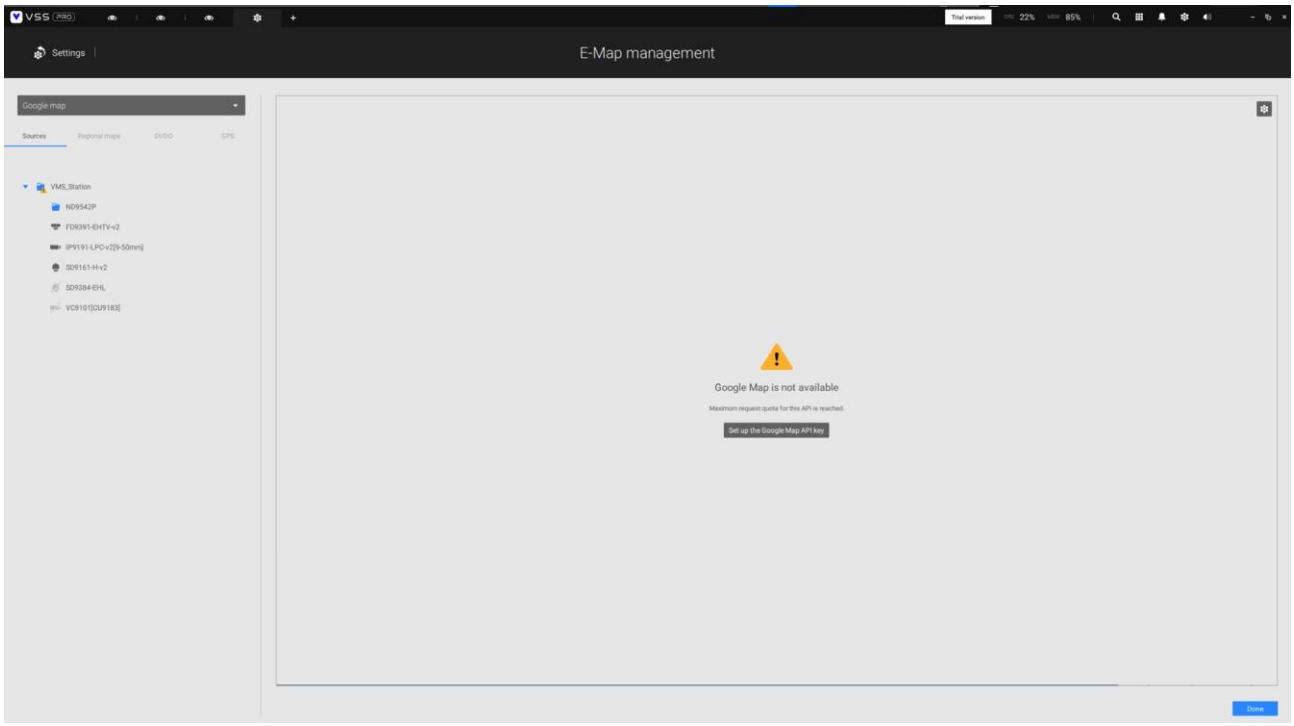


Configuring GIS or Google Maps and GPS

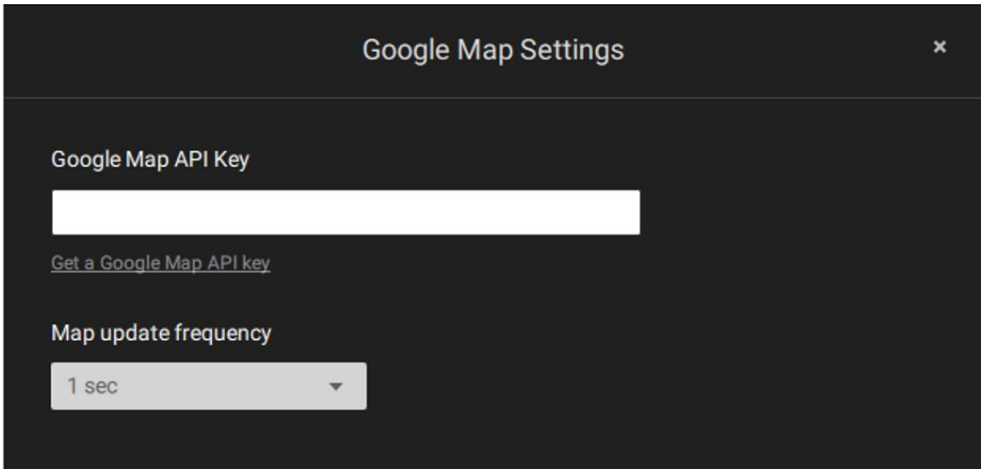
Since Google Maps changed its access policy, using the Google Maps feature requires a user to enter a billing API key. Using Maps, Routes, and Places APIs requires an API key.

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

Visit Settings > E-map > All Maps.



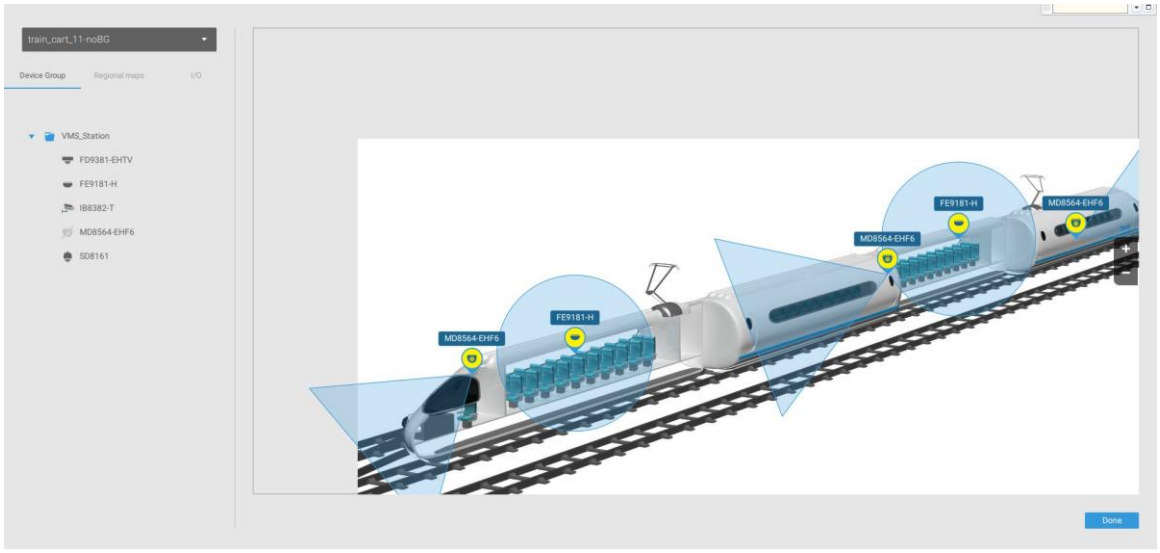
Enter the Google API key you previously registered (if using Google Map).



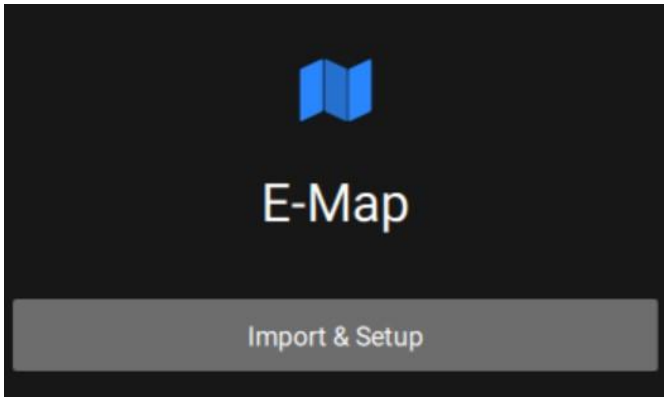
NOTE: In this revision, Google Maps only supports installation on GPS-enabled vehicles. Placing cameras in a static location on Google Maps is currently not supported.

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 into the database, the VSS 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.

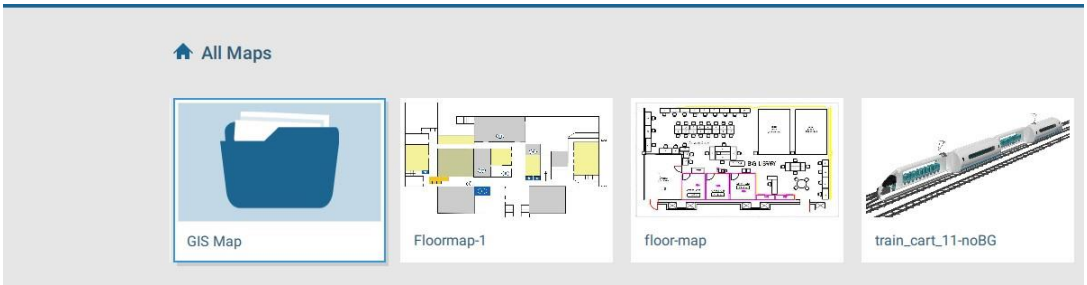
This applies to a mobile NVR that comes with GPS functionality.



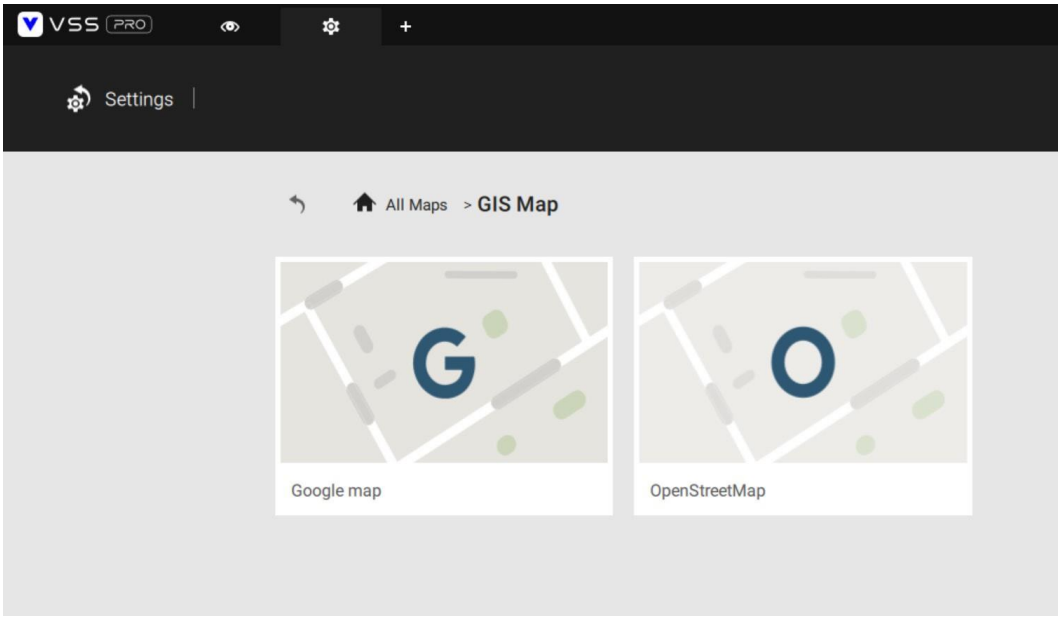
Open the E-Map Import & Setup window.



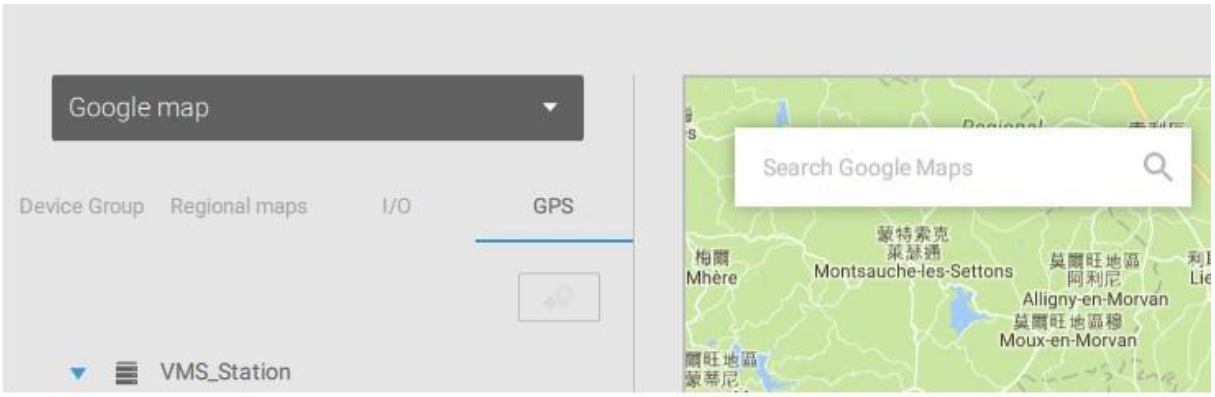
Click to enter the GIS (Geographic Information System) Map and then Google Map window.



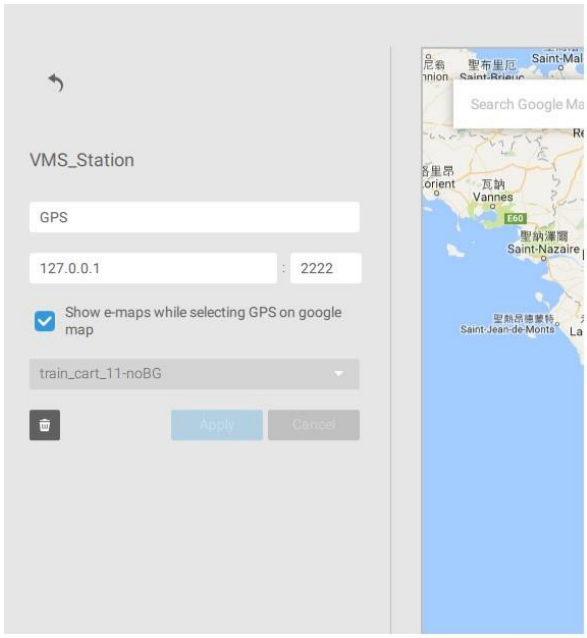
Click on either the Google map or the OpenStreetMap.



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

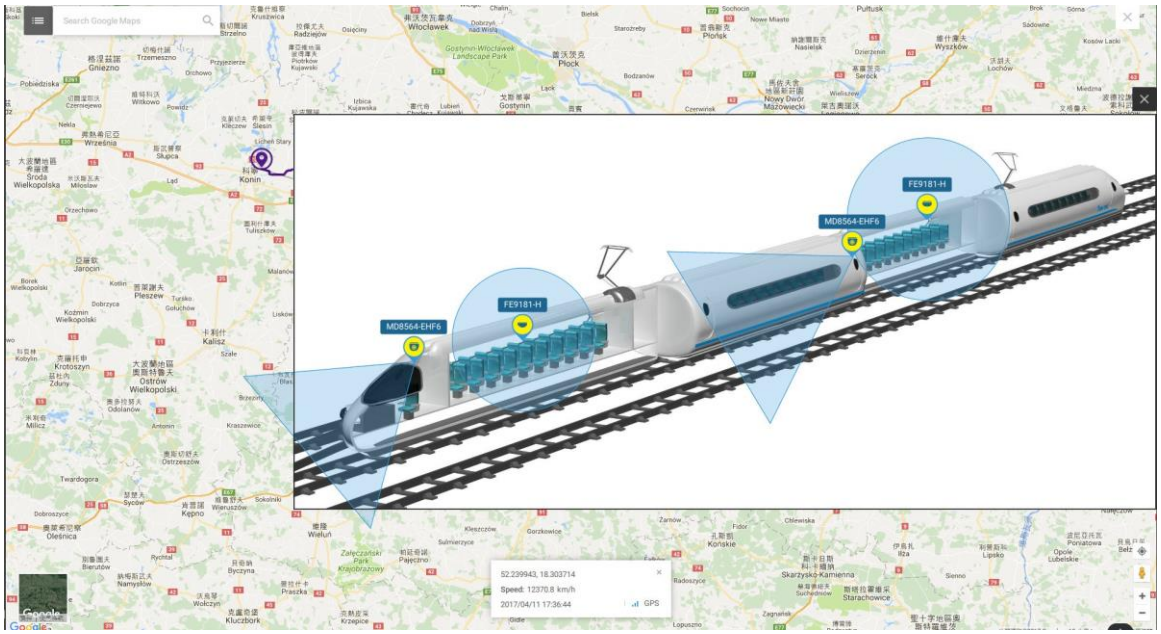


Enter a name for the GPS/GNSS server on the vehicle, its IP address, and server port number. You can select an E-map that will display when you click on the GPS location icon. Select the checkbox and an E-Map that corresponds to the deployment on the vehicle. When done, click the Apply button.



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 are also displayed on the map.



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

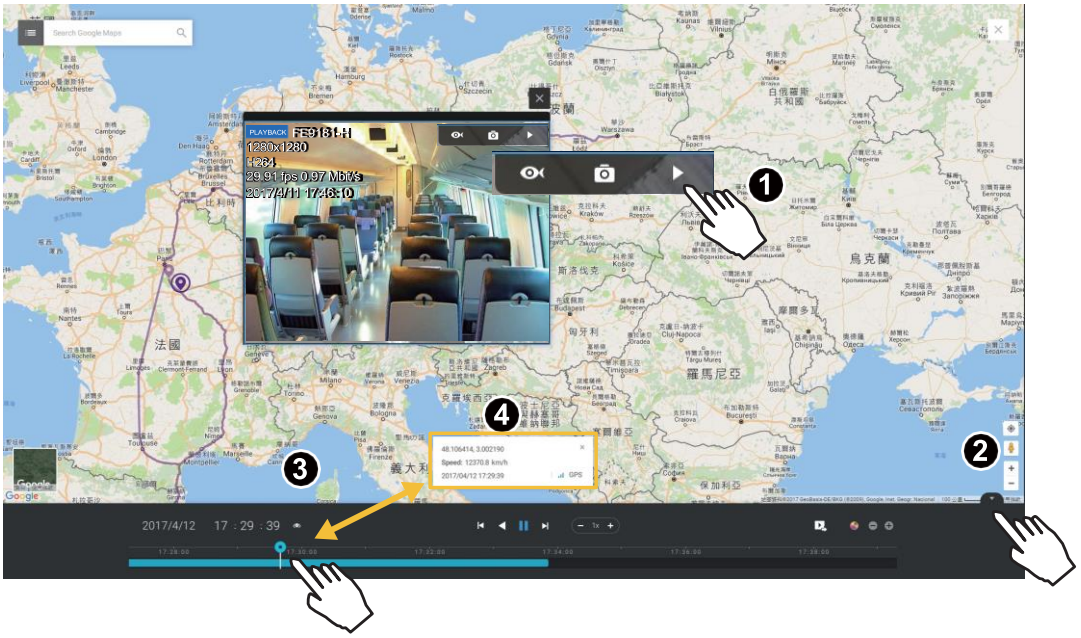
To search and review recordings when an event occurs,

1. Click on the Playback button.

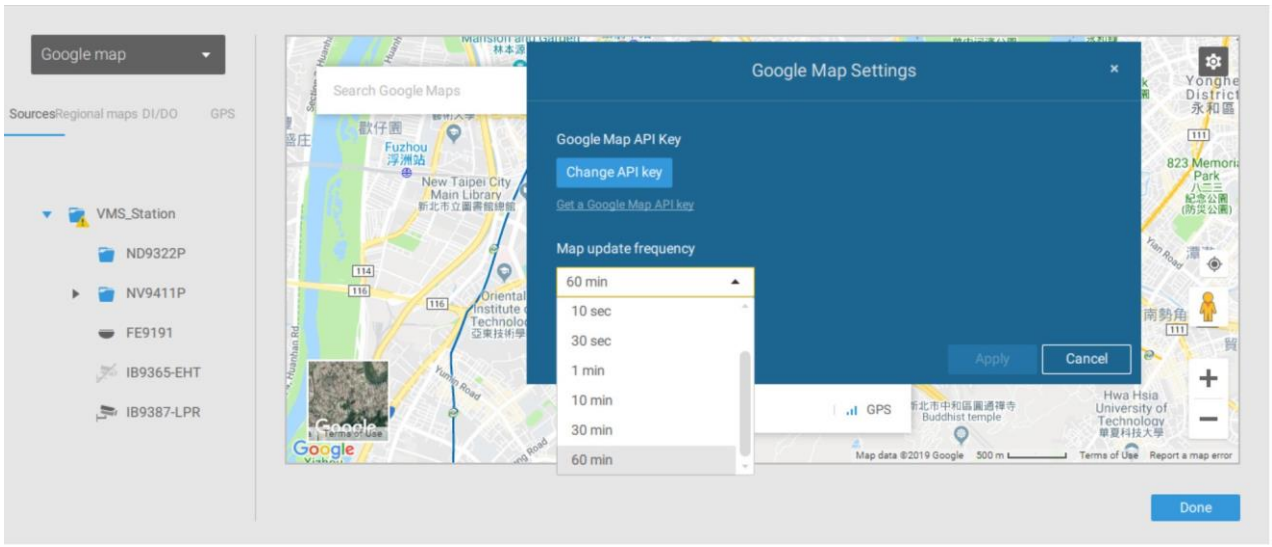
2. Click the Pane button to display the Playback control panel.

3. To search for the video of past events, pull the Playhead to a point in time on the timeline.

4. The GPS coordinates and time will change to those corresponding to the time you selected. You can then acquire the corresponding location information while tracing the occurrence of an event.



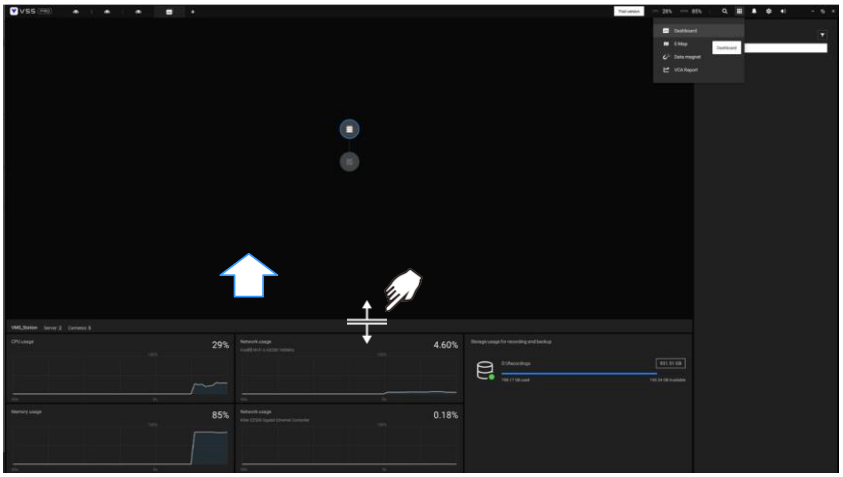
Click on the Setting button on the map to bring up the Map update frequency option. Your GPS target may travel to the outside of the map through time without the map being updated. The map will update by the interval you configure here.



2-15. 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.



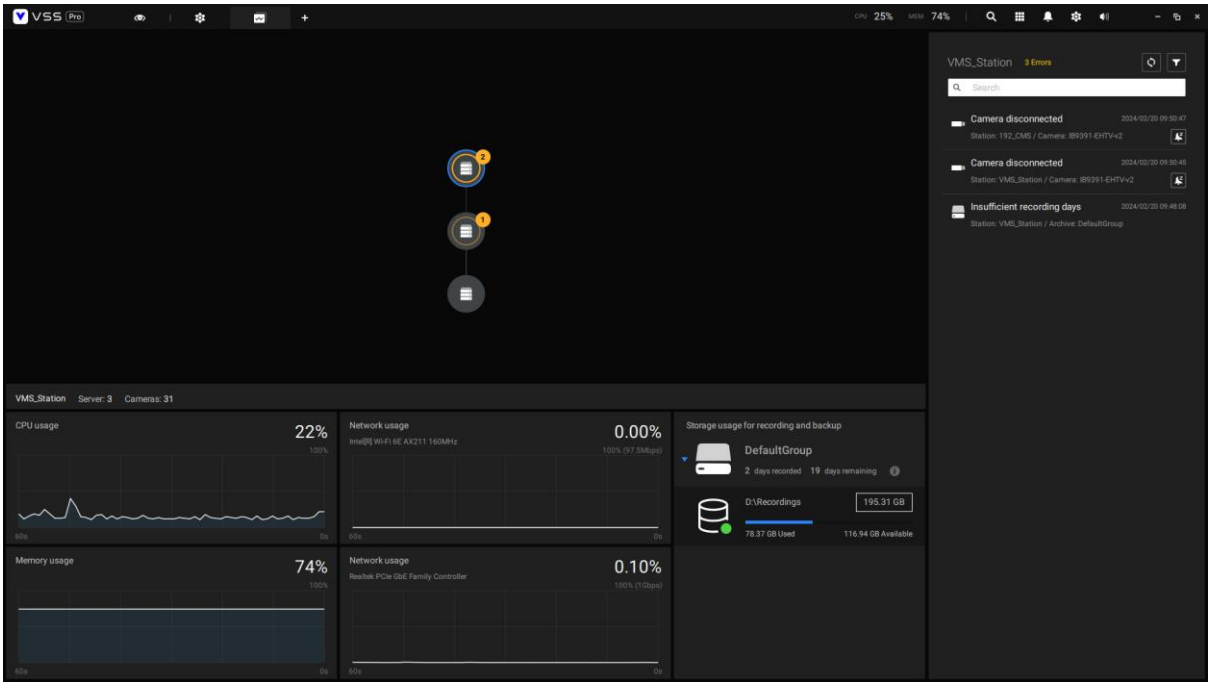
The possible system abnormalities can be:
CPU utilization over 90%
Memory usage over 90%
Network usage over 90%
Camera disconnected
Station disconnected

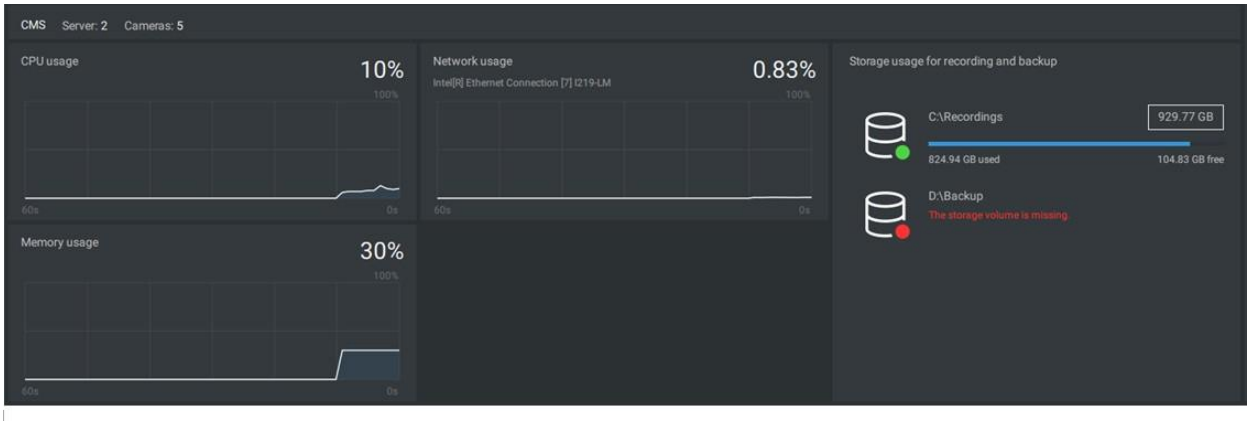
If you have multiple LAN cards or virtual HBAs, the status row can be pulled to reveal all of their statuses.

The "Storage Usage for Recording and Backup" panel displays information for each recording group, showing the total recorded days and estimated remaining recording days based on current storage capacity. It also provides details about storage volumes, indicating their capacity and usage size.

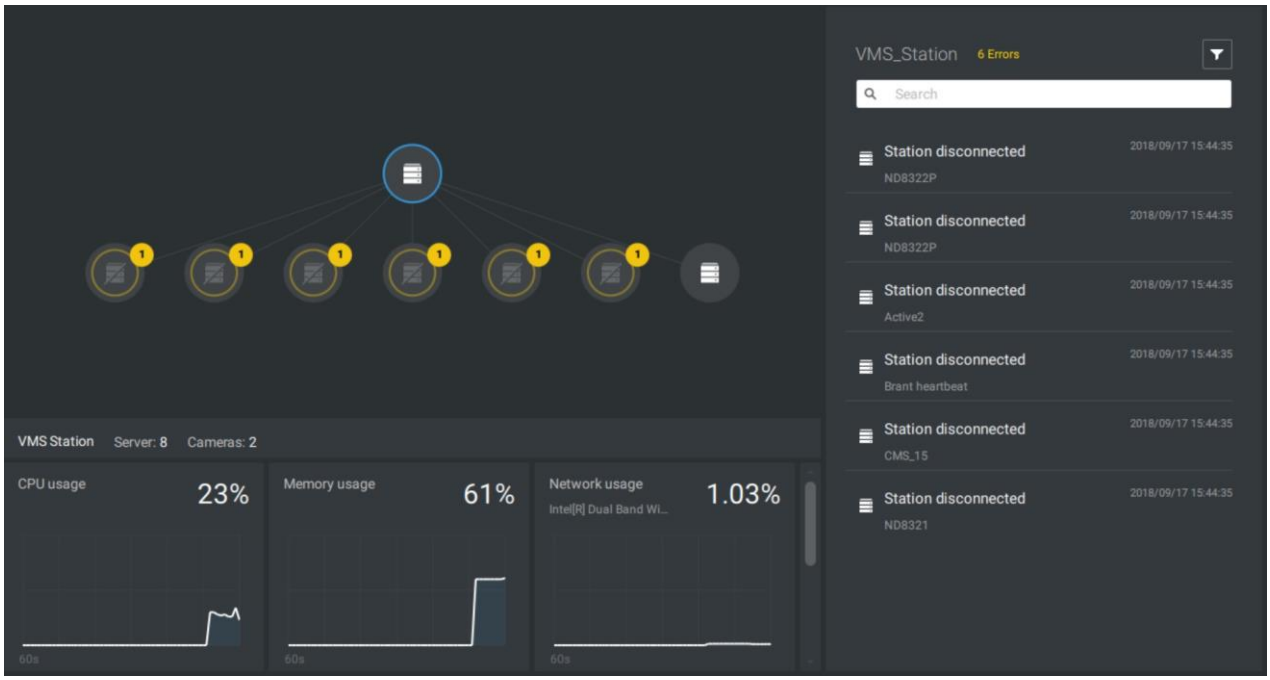
Notifications appear on the dashboard's status panel if a storage volume goes down or disconnects or the sum of estimated remaining recording days and recorded days falls below the user-defined retention days in the Recycle Option.

Note: The estimated remaining recording days are a rough reference calculated from the previous day's usage. Due to daily variations in recording content and camera configurations, consider it an approximation.

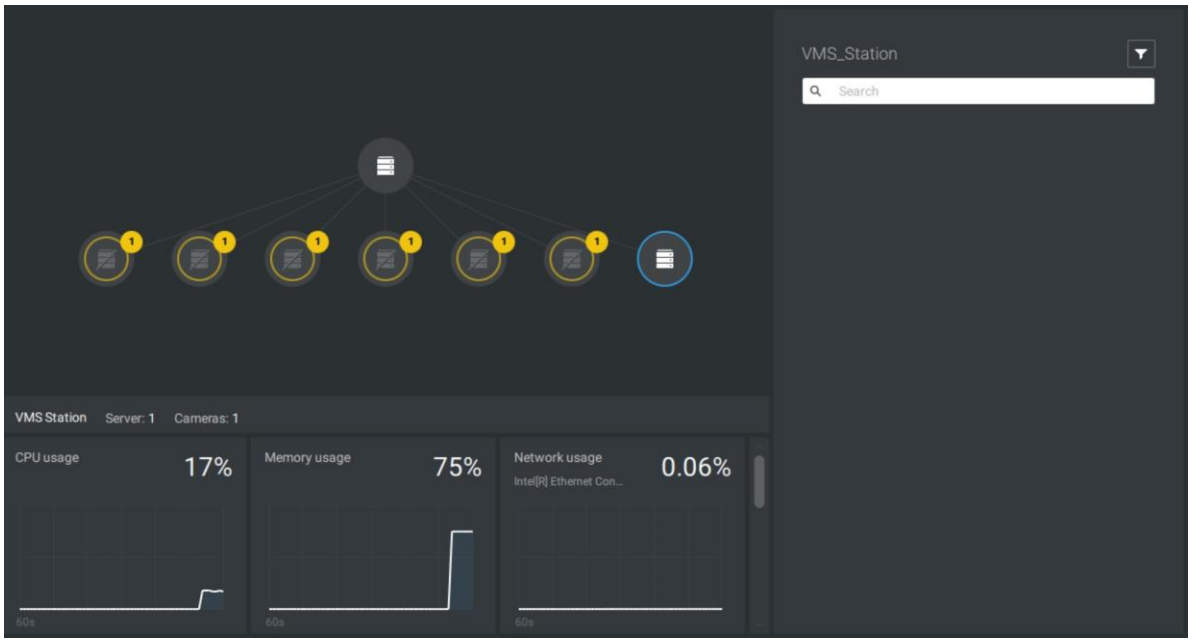




If you have multiple sub-stations, single-click to select and reveal their individual status, including CPU usage, memory usage, network usage, and storage usage.



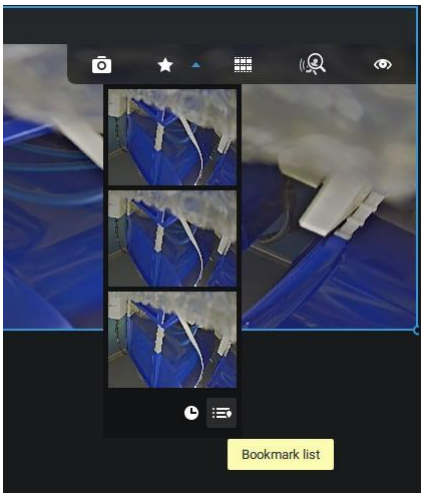
Note that VSS servers of the earlier revisions and NVRs running older firmware do not deliver their statuses to your Dashboard.



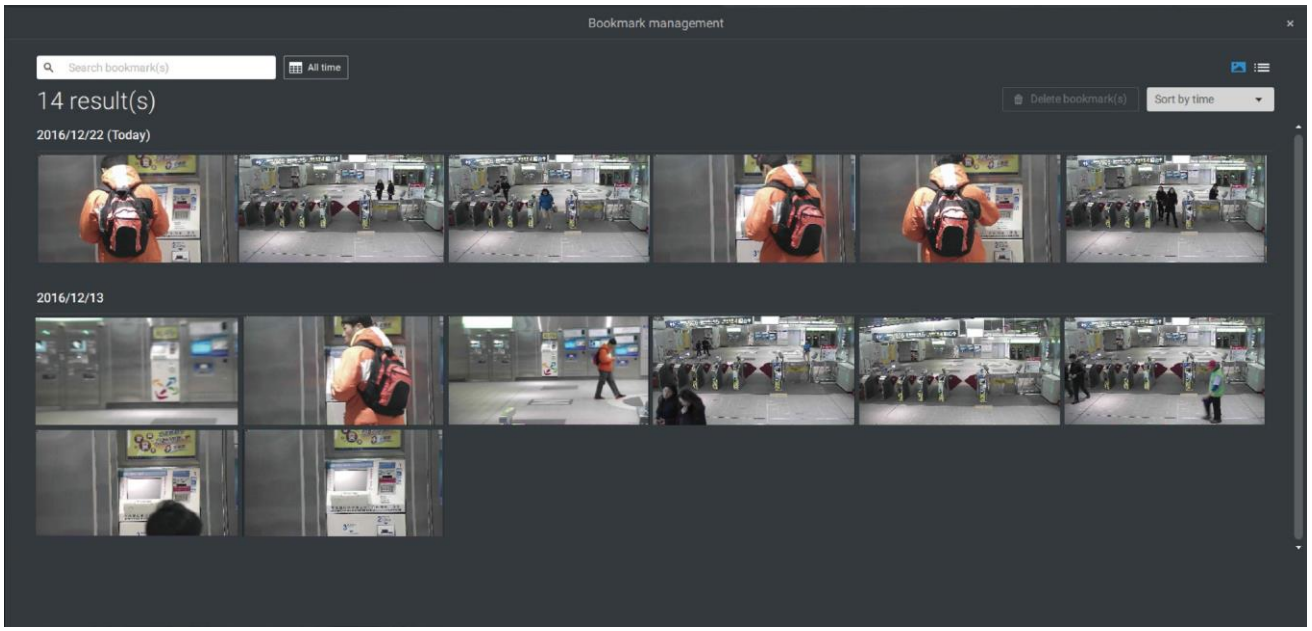
2-16. Search Panel

The Search panel is accessed via the Search button. 4 key functions are provided: **Bookmark search, Deep Search, Event search,** and **Smart search.**

1. **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.

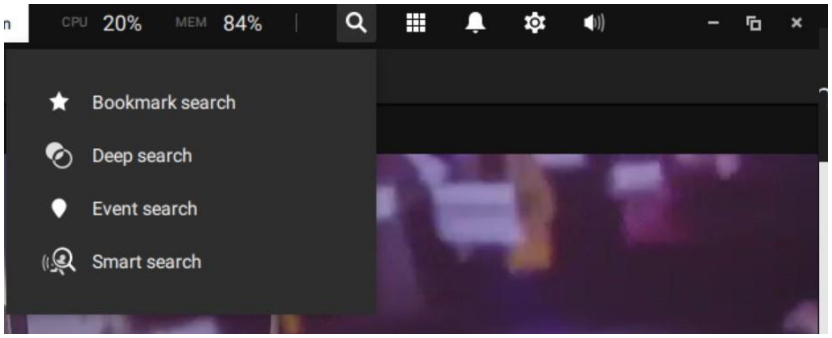
c. To remove an existing bookmark, left-click to select an entry, and then click the Delete bookmark(s) button. Bookmarks will be indicated as "Invalid" if the videos where the bookmarks were appended were erased, e.g., when the original recording was erased by cyclic recording.

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.

2-17. Event Search

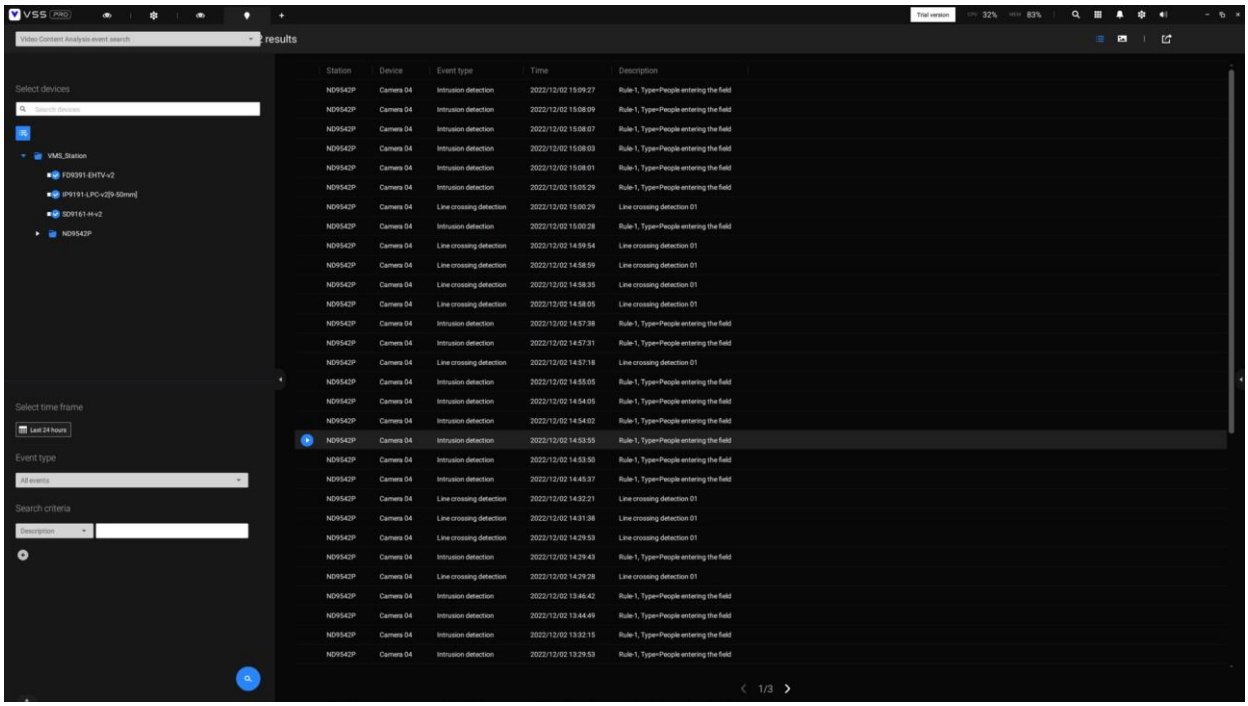
The Event Search window is accessed from the top toolbar.



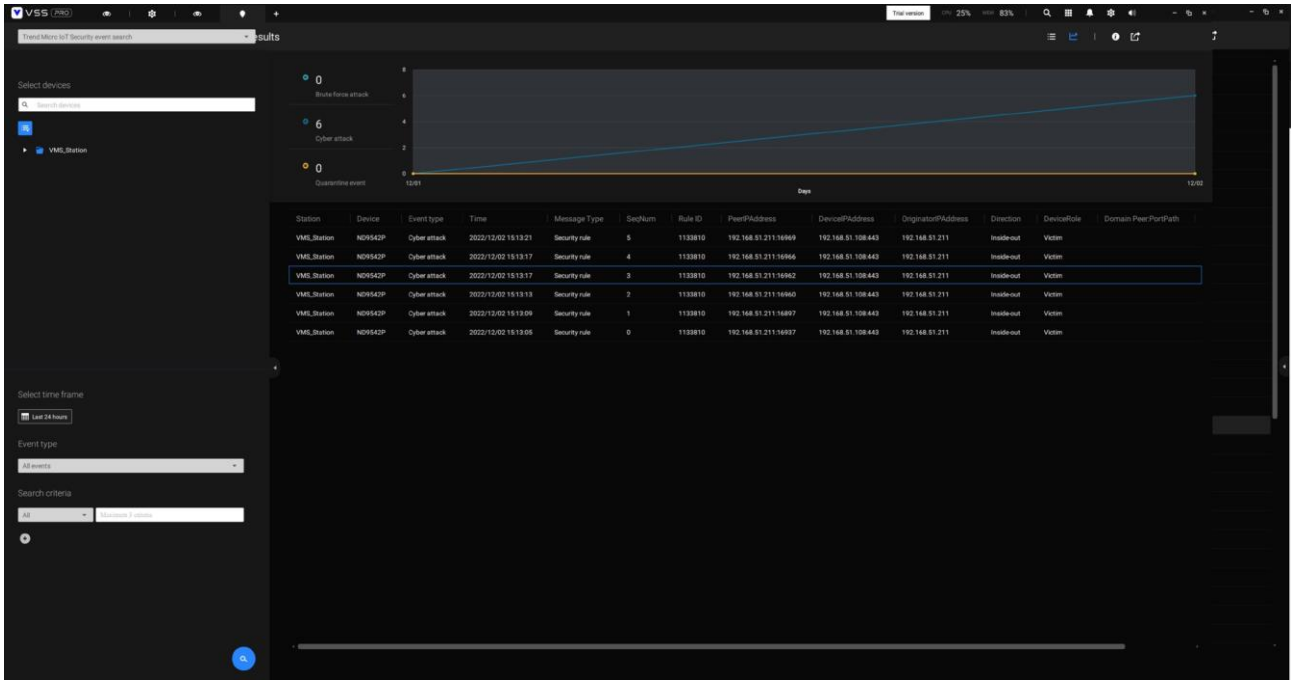
Below is the comparison between the Alarm list and the Event search windows:

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.

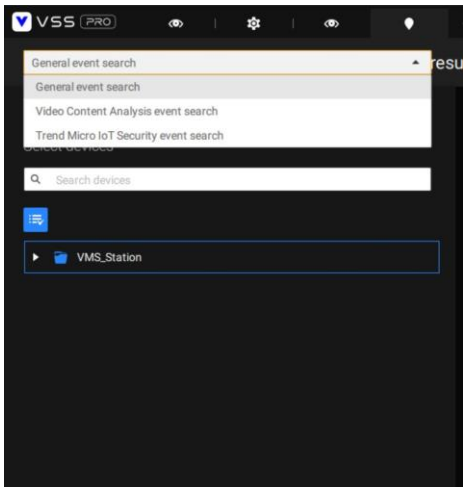
The sample screen for VCA-related events is shown below:



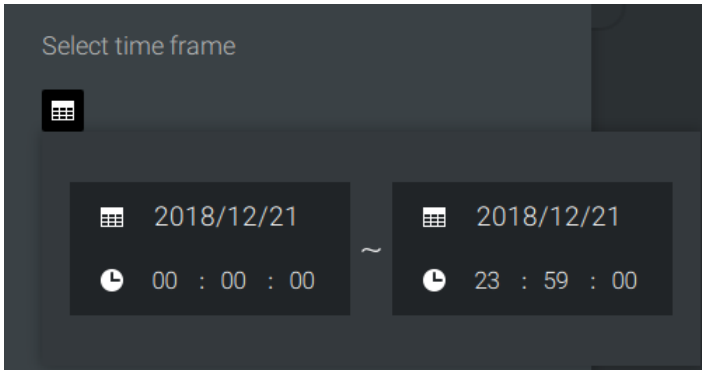
The sample screen for network security-related events is shown below:



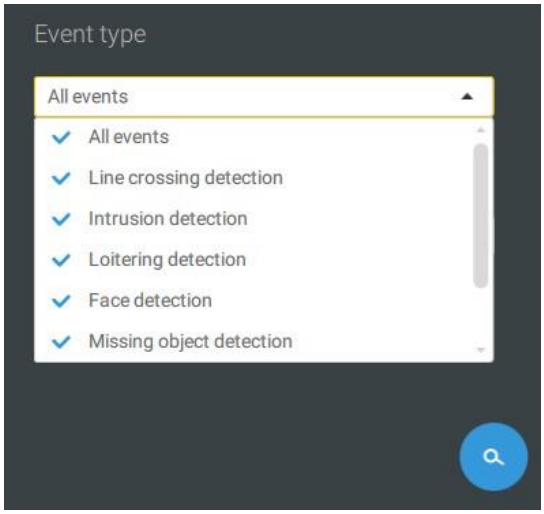
From the Search Event window, you can view and search events by their event types and use the Export button to save a record of these events (in the CSV format).



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



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



Click the search button to generate search results.

2-18. Thumbnail search

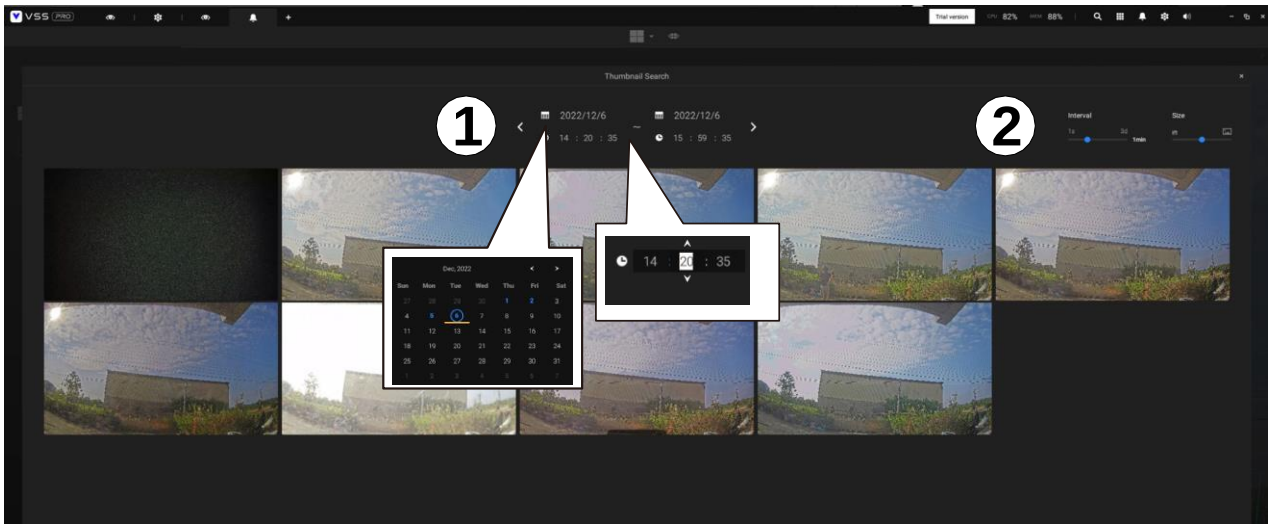
The Thumbnail search function is like doing a post-production editing in film making. Screens from across different time spans are shown to facilitate the search for evidence.

VSS 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,

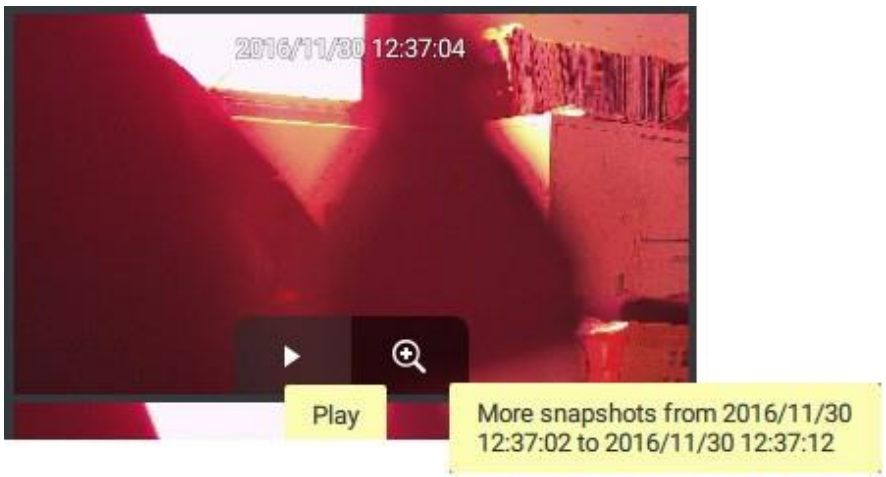
1. Use the date and time selectors to specify a time span during which you suspect the event of your interest has occurred.
2. If preferred, tune the interval and clip size. The default length for each clip is 10 seconds.
3. If you find a clip might contain an event of your interest, you can click to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



2-19. Smart search

The Smart search function enables a quick glimpse of activities that occurred within a user- 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.

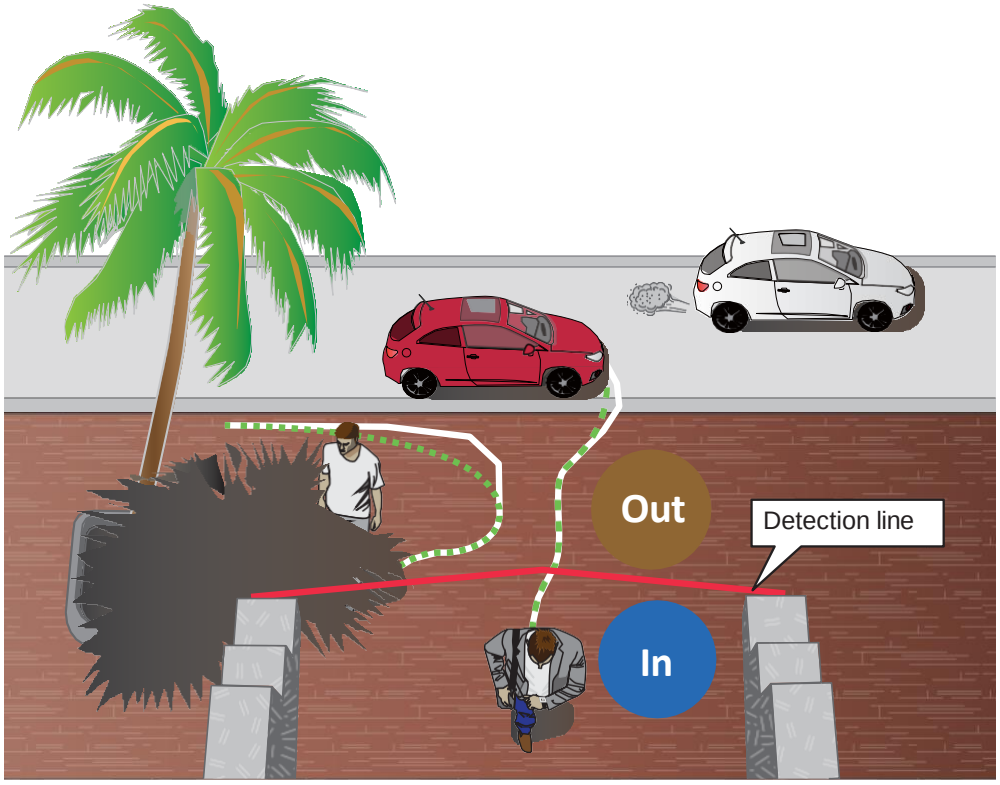
Please refer to VIVOTEK's website pages that are related to the Smart motion and Smart VCA features for the supported cameras.

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

Below is a 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 the screen for persons passing the line in one specific direction or in both directions.

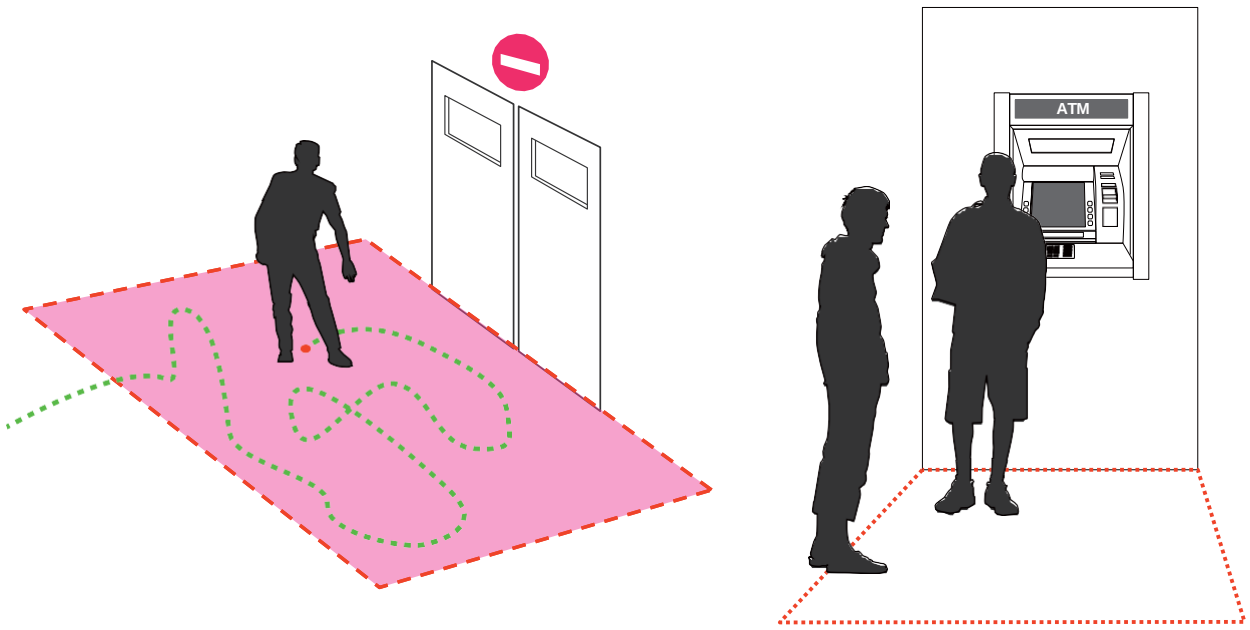


The applicable scenarios of this feature can be:

* Detects someone who enters a driveway, 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.

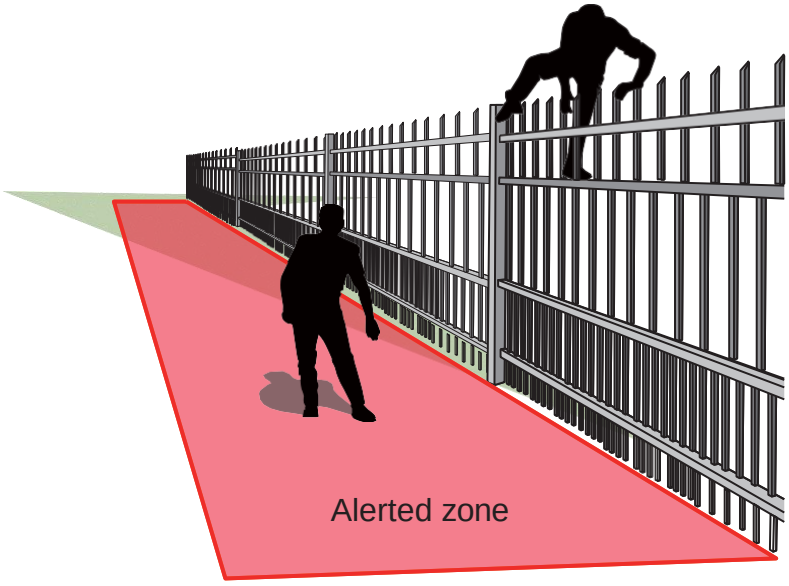
Loitering Detection

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.

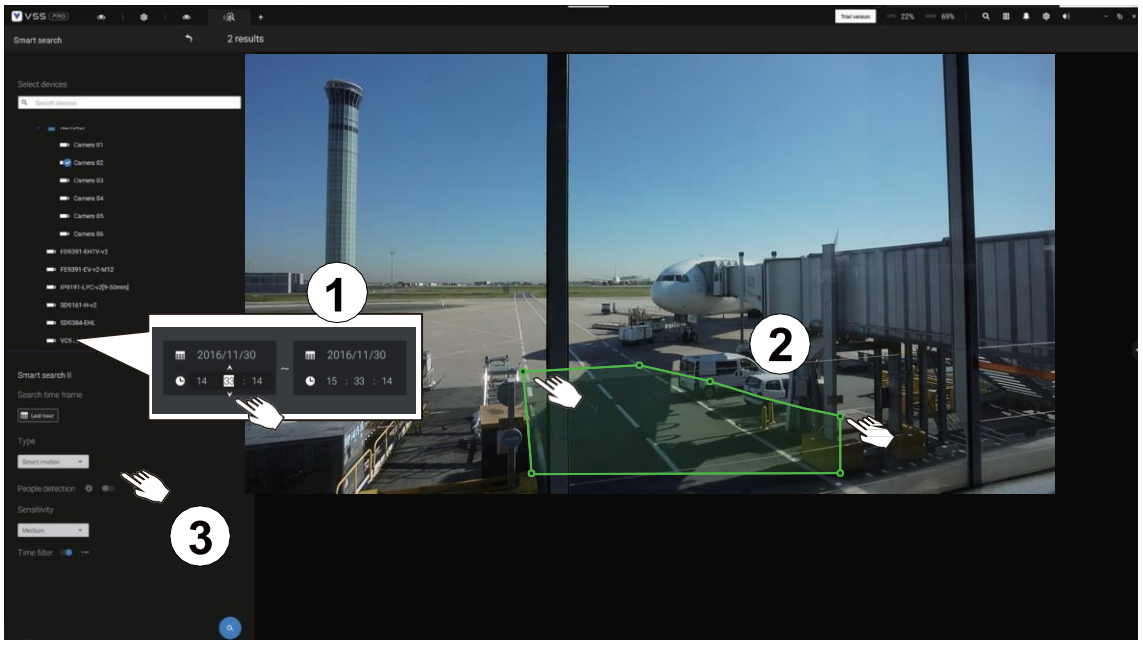


The applicable scenarios of this feature can be:

* 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.

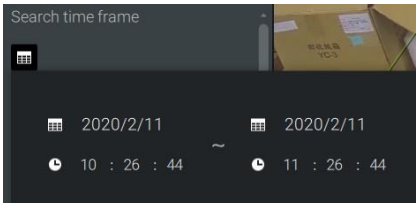
To use Smart search,

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:

<table>
<tr><td>Search time frame</td><td colspan="4">Use the calendar tool pane to specify the time span within which the activities in scene will be searched.
 
</td></tr>
<tr><td>Type</td><td colspan="4">If the selected camera supports multiple Smart VCA detection features, the supported types will be listed:
Smart motion, Line crossing, Loitering, or Intrusion.</td></tr>
<tr><td rowspan="4">Parameters
(determined by Type)</td><td>Smart motion</td><td>Line crossing</td><td>Loitering</td><td>Intrusion</td></tr>
<tr><td>People detection*</td><td>People walking direction</td><td>Stay time</td><td>Direction:
Into the zone /
Leaving the zone</td></tr>
<tr><td>Sensitivity**</td><td></td><td></td><td></td></tr>
<tr><td>Time filter</td><td></td><td></td><td></td></tr>
<tr><td></td><td colspan="4"></td></tr>
<tr><td>* People or Vehicle detection</td><td colspan="4">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.</td></tr>
<tr><td>** Sensitivity</td><td colspan="4">Configure the sensitivity for the detection of the activities in a scene. Low for near scenes, high sensitivity for long-distance scenes.</td></tr>
</table>

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.

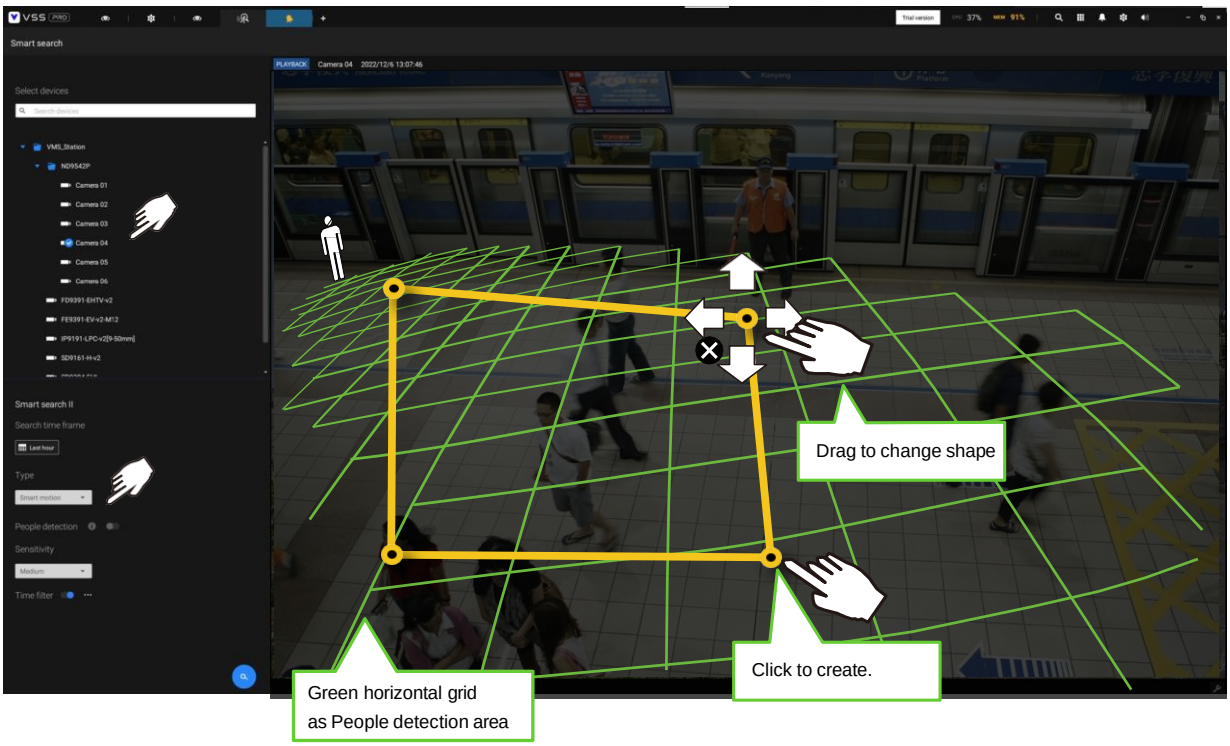
NOTE:

* 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 VSS 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.

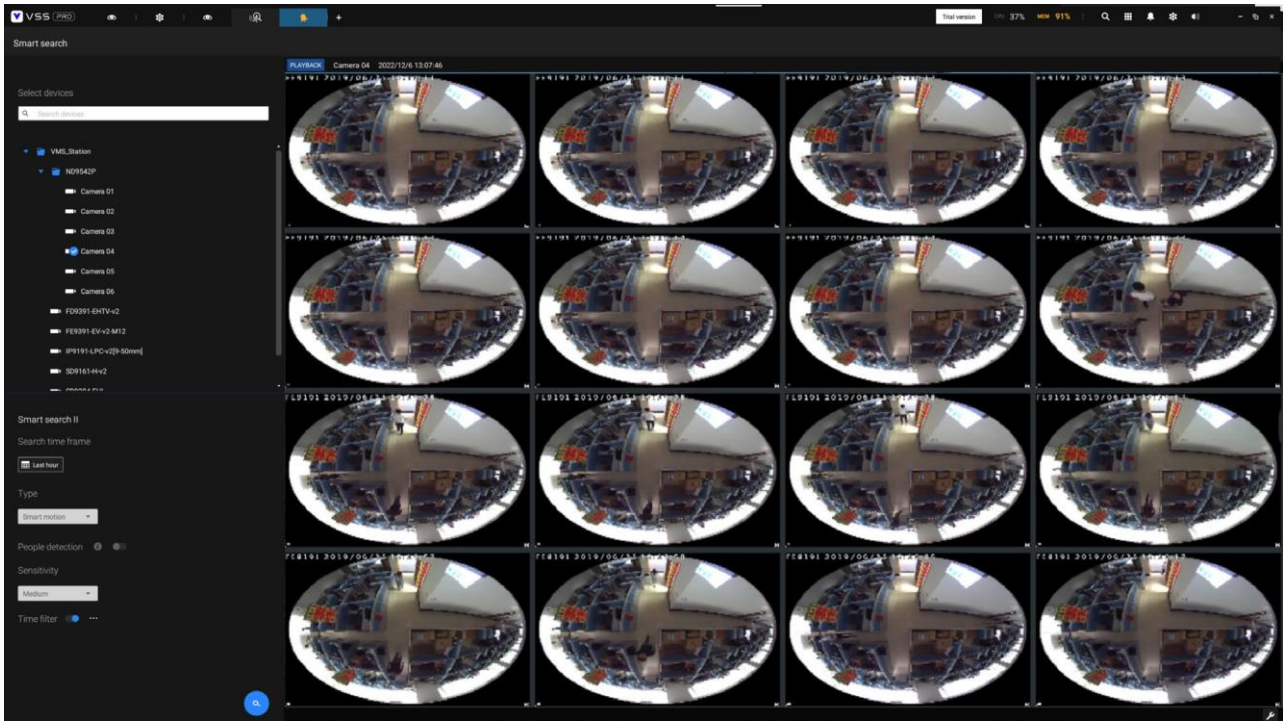
1. Select a VCA camera.
2. Select a VCA type from the pull-down list: Smart Motion, Line crossing, Loitering, or Intrusion. For a camera that supports only one VCA feature, such as Smart tracking on a speed dome, there is no "type" option.
3. You can then draw a detection zone, or detection line on the 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.



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.

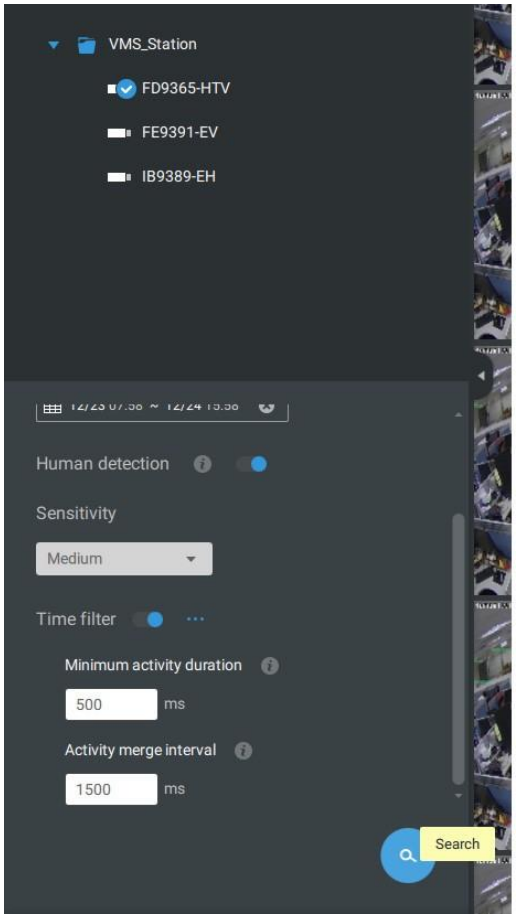
   Hover the screen with your mouse, and the length of each video clip is displayed.

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



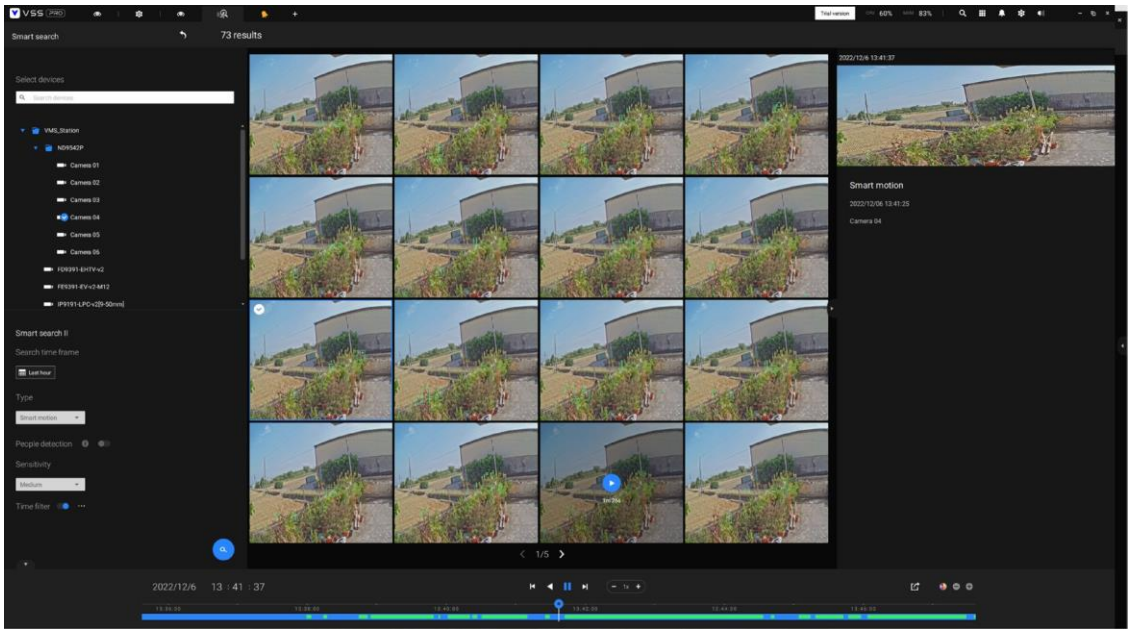
Smart search II is available only for newer line of cameras that come with Smart Motion detection and other Smart VCA features. Smart search II has the following benefits:

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 VSS search panel screen.

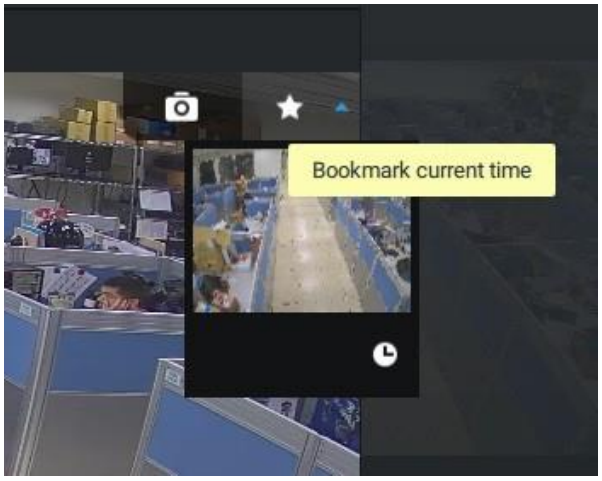


You can specify the time span, People detection, Sensitivity level, and time filter parameters in a Smart Search II panel.

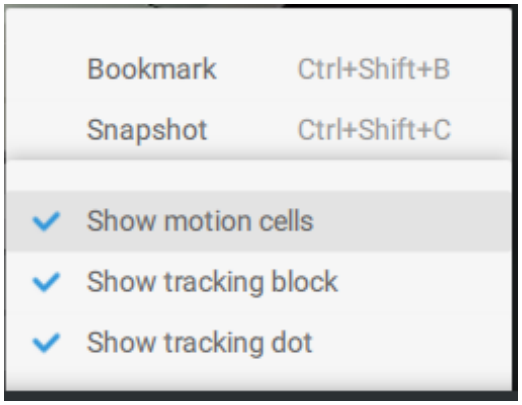
5. You can then click to open any clip of your interest. Each marked event clip will be indicated by a lighter color on the timeline. Select and double-click on a video clip, and then right-click or select the bookmark or snapshot functions from the upper-right.



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.

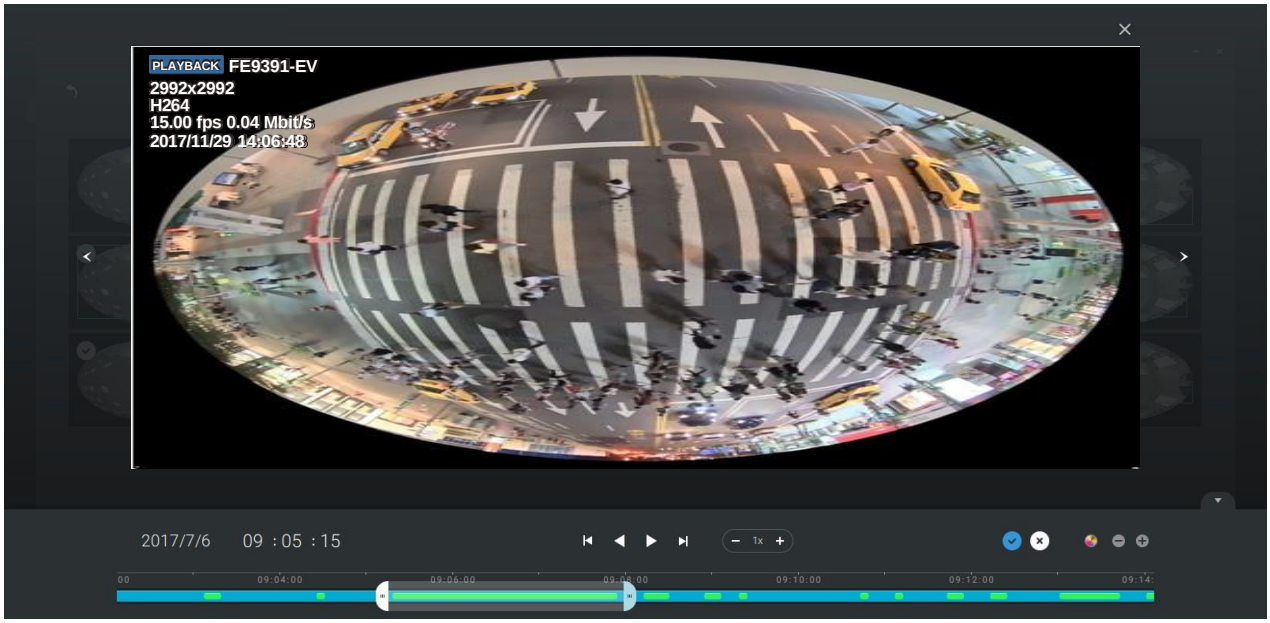


While in the full-screen Playback window, you can right-click to select or deselect the display elements including motion cells, tracking block, and tracking dot.

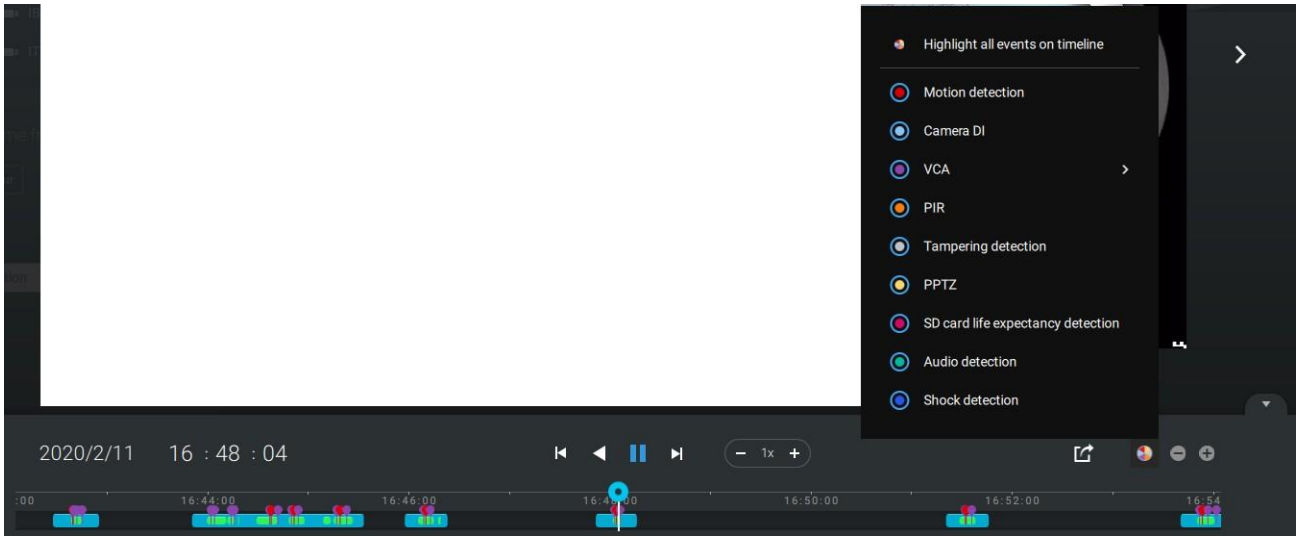


6. If you find important events, use the Export function to mark the start and end points on the timeline to export a video clip. Use the pull tabs on time line to determine the export length. By default, the export length is 2 minutes long.

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



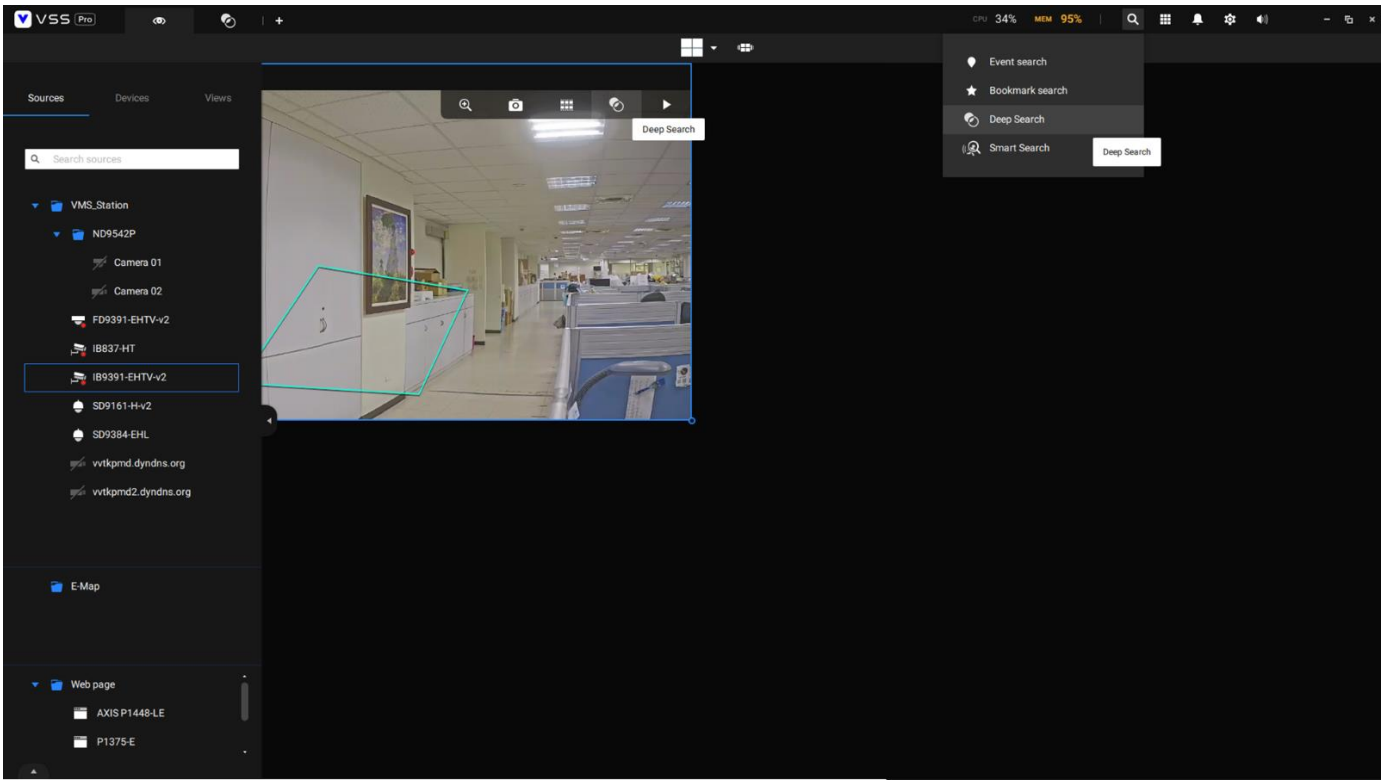
   Different events on the timeline are indicated by tags of different colors. Click on the event highlights button to verify their colors.

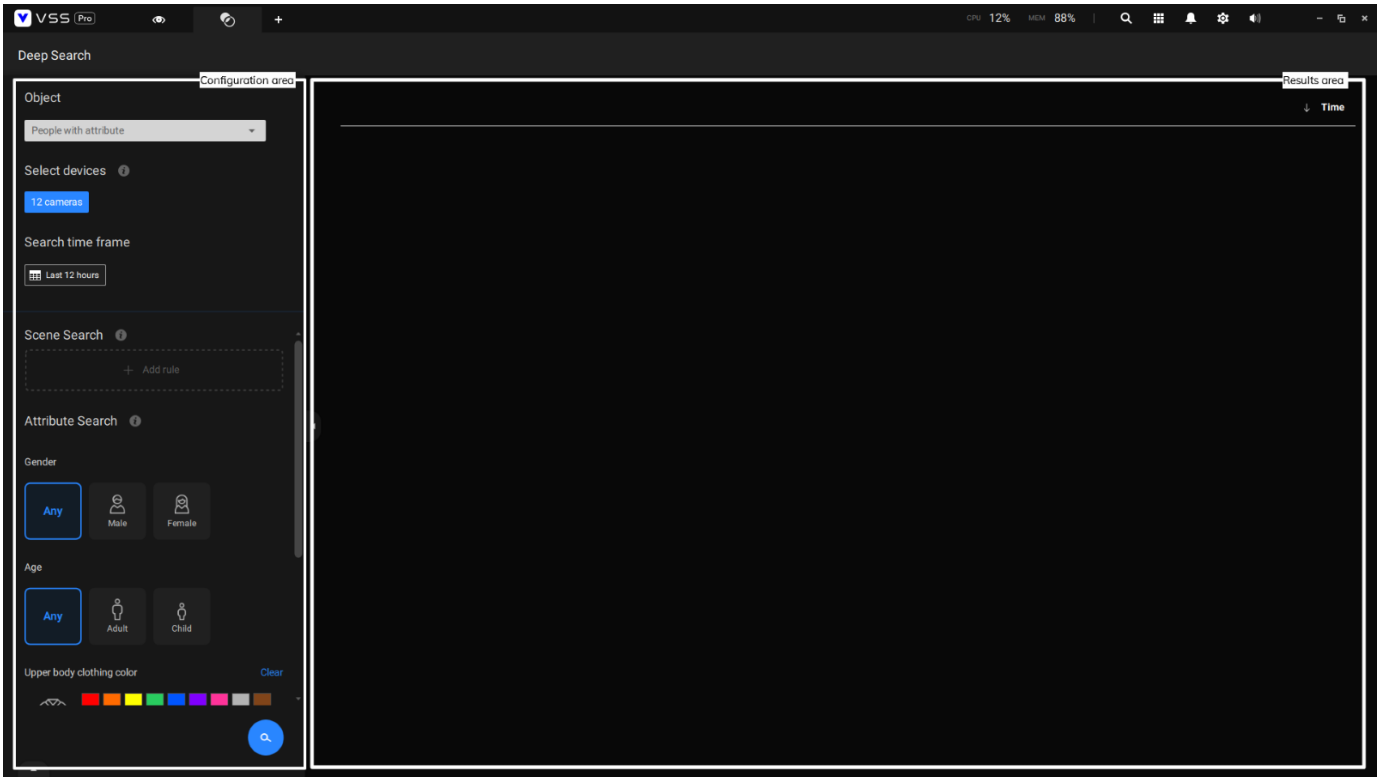


2-20. Deep Search

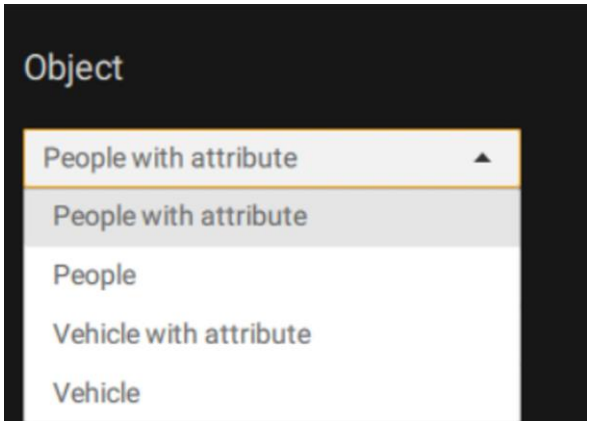
The Deep Search function uses AI empowered by VIVOTEK AI cameras to improve search functionality, and it comprises three main functions: Attribute Search, Scene Search, and Re-Search (VSS Professional edition only). Without relying on scrolling through the video footage frame by frame, VIVOTEK AI cameras provide object-based metadata to enable intelligent video evidence search. By utilizing object-based metadata-defined attributes and rules, Deep Search helps users search for the target of interest smarter and faster.

To use the Deep Search function, make sure you have enabled the Deep Search function, added the cameras that support Deep Search, and have the time synchronizing among the VSS client, VSS server, and cameras. There are two ways to access the Deep Search function; one is to click the search icon and select Deep Search, and the other is to click the associated icon  on a live view cell.

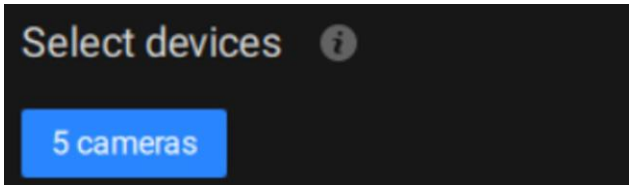



VSS Pro
CPU 12% MEM 88%
Deep Search
Configuration area
Object
People with attribute
Select devices
12 cameras
Search time frame
Last 12 hours
Scene Search
Add rule
Attribute Search
Gender
Any
Male
Female
Age
Any
Adult
Child
Upper body clothing color
Clear
Results area
Time

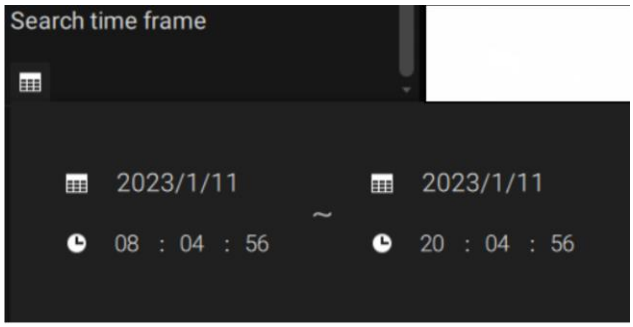
Select the object type in the configuration area, including people, vehicle, people with attribute, and vehicle with attribute. Select people or vehicle objects if you want to search for people or vehicles in the recorded video. Select people with attribute or vehicle with attribute if you want to find people or vehicles and know their appearance.



Note that not all cameras support finding all the object types. When users select one type of object, only the supported cameras will appear in the camera list.
By default, all the cameras that support the object type will be selected. Users can click the device list and choose the cameras.

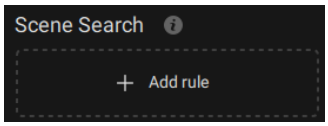


Select a time frame using the pull-down menu.

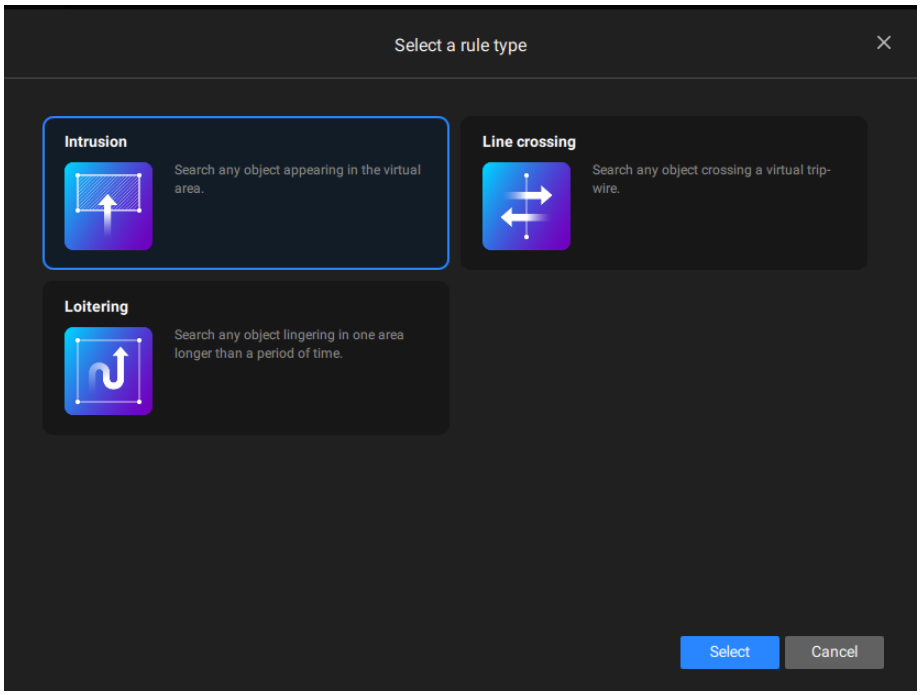


Select Scene Search or Attribute Search.

Scene Search

Search for the object appearing or lingering in the virtual area or crossing a virtual tripwire. Note that this search can only be used if you select a single camera. Users can click the 

button to select a search rule type.



- **Intrusion:** Draw a closed area in which you want to find related people or vehicles staying in this virtual area.
- **Line crossing:** Move the nodes to draw a tripwire to find related people or vehicles crossing this virtual wire.
- **Loitering:** Draw a closed area in which you want to find related people or vehicles staying in this virtual area for more than a specified period.

If there are search results after performing Deep Search, you can play each corresponding video thumbnail and take snapshots as needed.

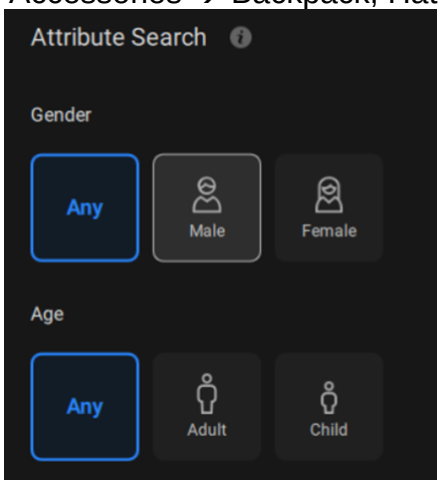
Attribute Search

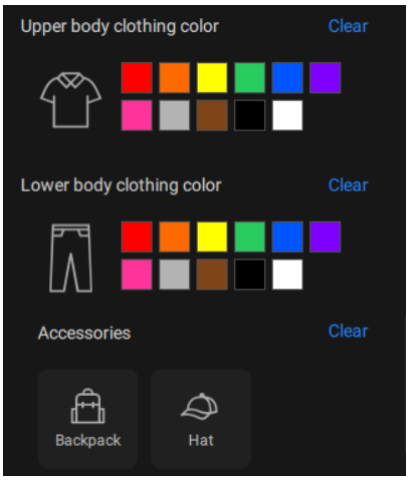
filter the object with selected appearance. Note that this search is only available when users select the people appearance or vehicle appearance object. The supported appearance for vehicle and people is listed in the table below.

Object Appearance:

- People with Attribute

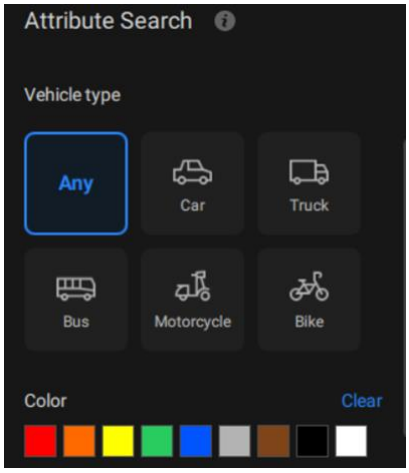
  People → Gender, Age, Clothing color
  Accessories → Backpack, Hat





- Vehicle with Attribute

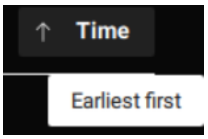
  Vehicle → Type, Color



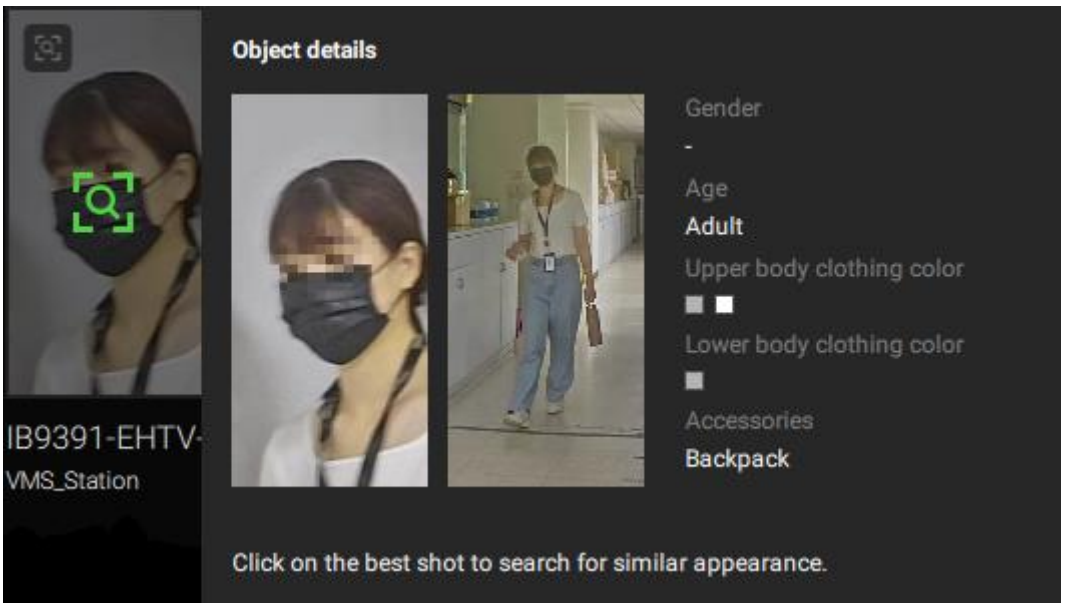
Click the search icon, and the results will display in the results area. The number of results will be shown at the top of the results area. Each result contains a snapshot of the object and a video clip of trajectory for the object, and user can click the video clip to playback the video. Also, users can click the sorting icon on the top-right of the results area to sort the results from the latest to the earliest or vice versa. If there are more than 200 search results, only the latest 200 results will be listed.

Hence, by default, the first 200 results will be listed if the time is sorted from the latest to the earliest.

The first 200 results will be listed if the time is sorted from the earliest to the latest.



VIVOTEK AI cameras with supported Deep Learning VCA package versions can capture and provide not only body snapshots and metadata but also face snapshots and metadata to VSS. Users can see object details, including snapshots and attributes, by hovering over a snapshot.



Re-Search (VSS Professional edition only)

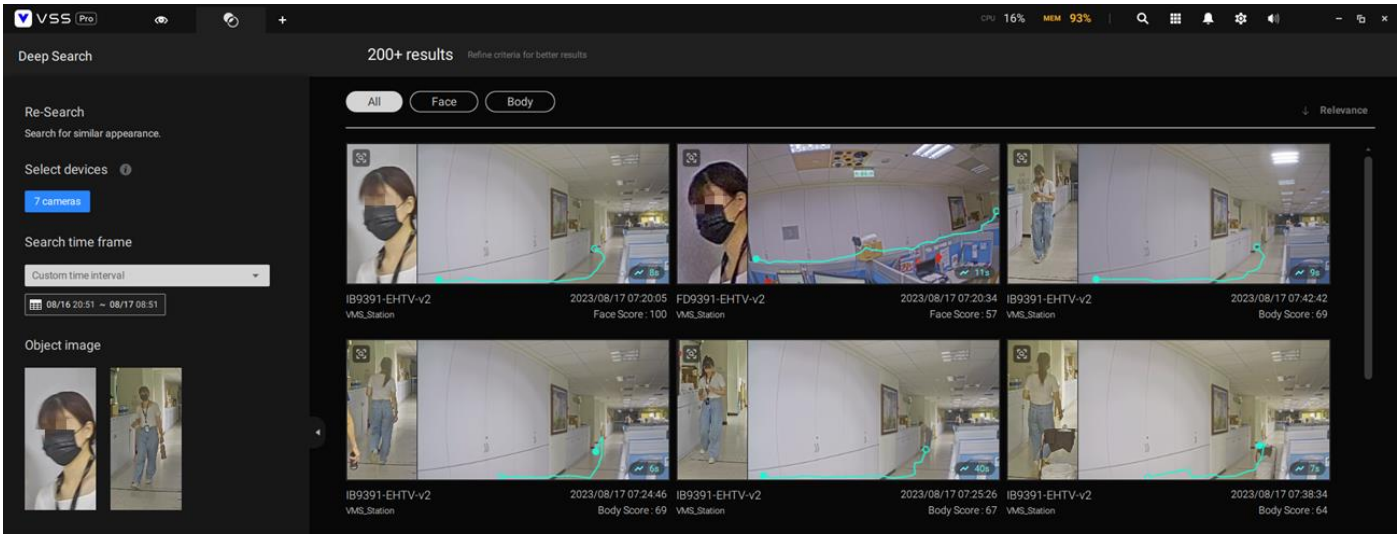
After all the search results shown by the above three filters, users can click the snapshot of the object to search for similar appearance. Users can select to apply Re-Search based on:

- Current selected device and time frame: Click “Search with current settings” to start Re-Search based on the currently selected device and time frame.

or

- Custom settings: Click “Search with custom settings” to start Re-search based on the re-selected device and time frame.

When Re-Searching the face snapshot of an object, the results will show both objects with similar faces and similar bodies in the descending order of similarity.

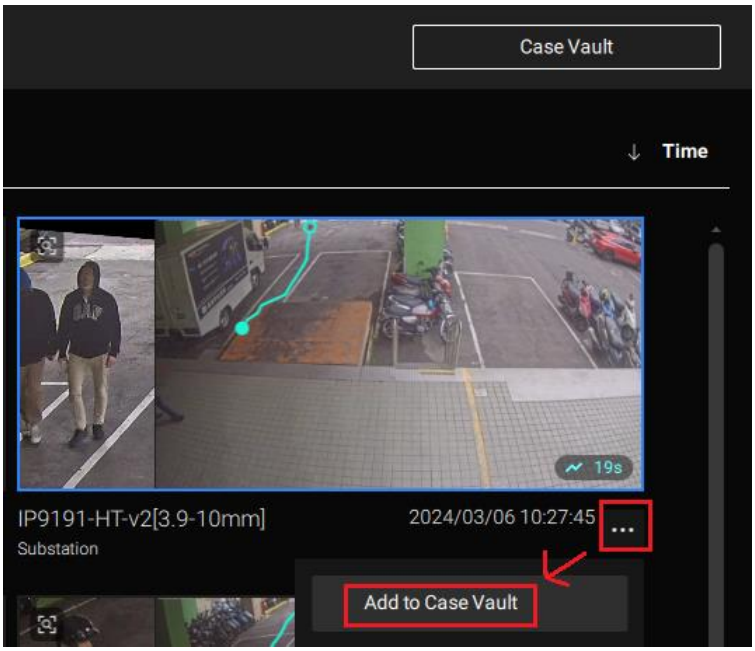


Case Vault (VSS Professional edition only)

The Case Vault function enables users to curate a personalized list of interested objects' video clips discovered through Deep Search. Once added to the Case Vault, the videos are organized chronologically for easy review and report generation.

How to Add Videos to the Case Vault?

Perform a Deep Search or Re-Search to find relevant video clips. In the upper right corner of each video clip, locate the "More" menu. Open the "More" (…) menu. Choose the "Add to Case Vault" option to include the video in the Case Vault list.



Case Vault Functions

1. Quick preview in Case Vault

   The added videos will be automatically arranged in the Case Vault based on the time of occurrence. Users can delete unwanted videos. Hover over the video screenshot in the Case Vault to play the video at double speed for quick previews.

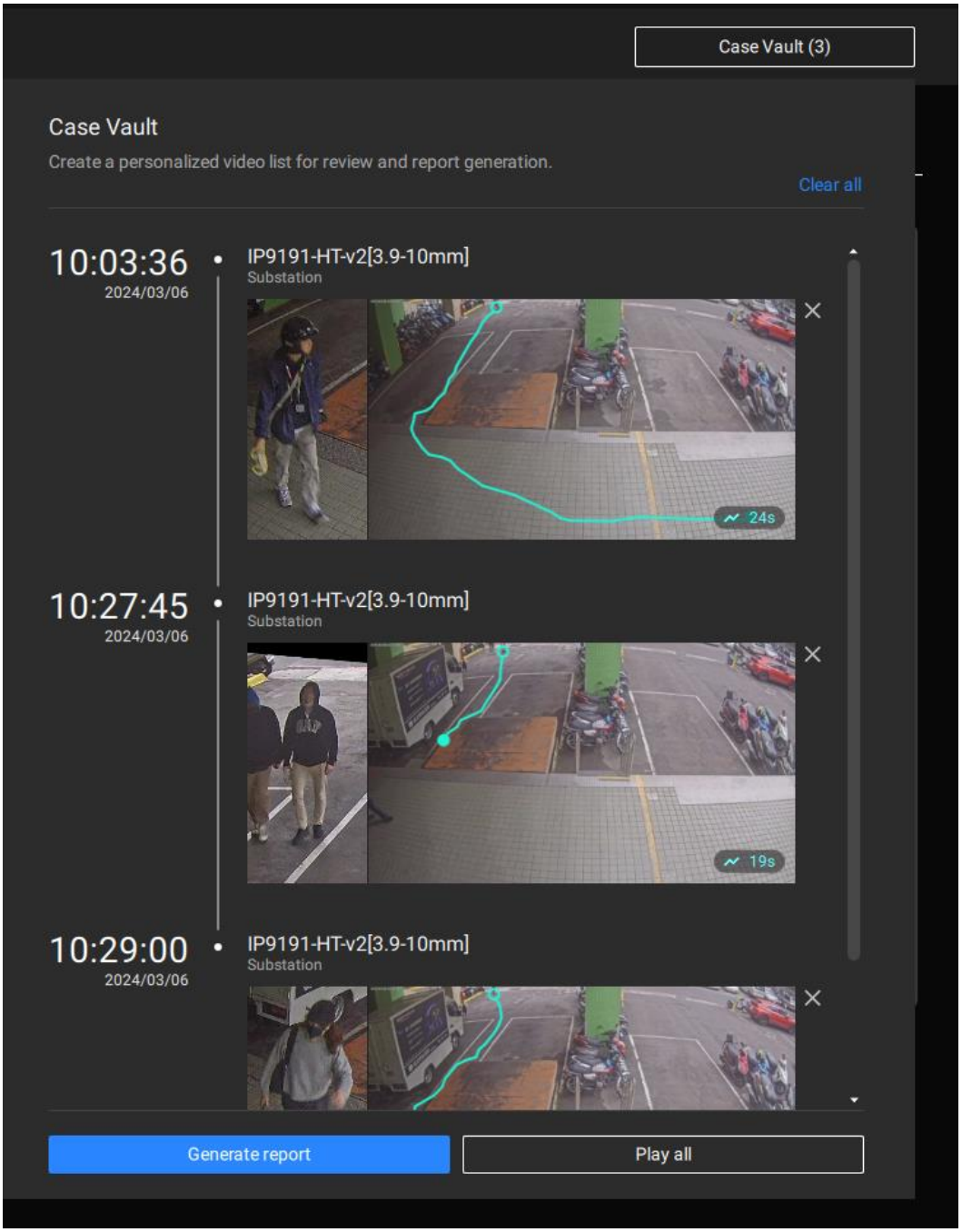
2. Case Vault Playback

   Click on the "Play all" button, and Videos will play in a larger screen format, seamlessly transitioning based on their chronological order. On the video playback control bar, click on the "Show related E-Map" icon to view the cameras associated with the currently playing video in their designated positions on the E-Map.

   Note: Only one E-Map will be shown if one camera is placed on two E-Maps.

3. Report Generation

   Automatically generate a comprehensive report based on the content of the videos in the Case Vault.

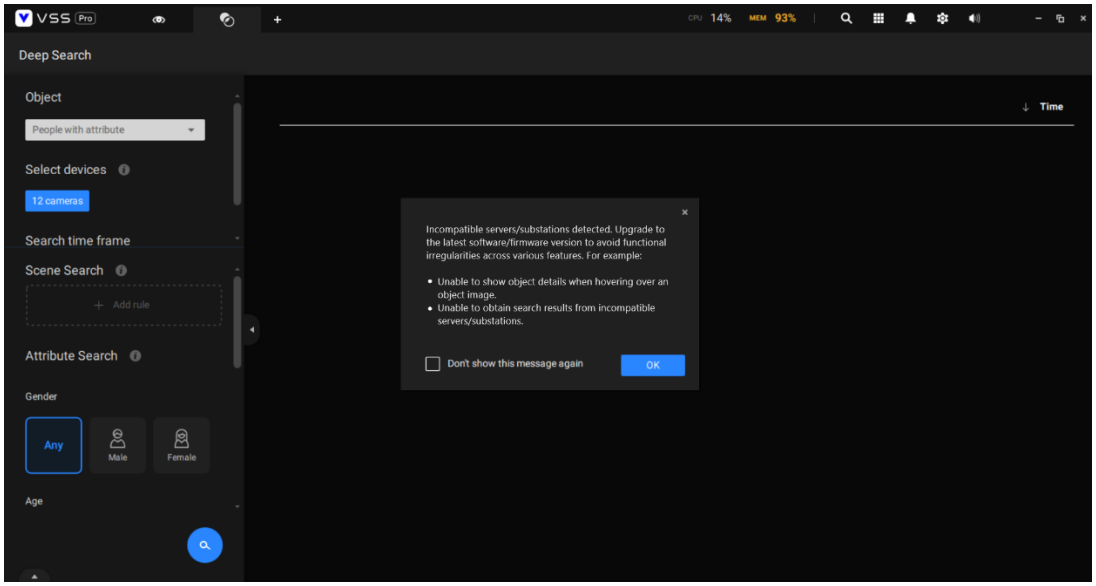


After reviewing the videos, click the "Generate report" button in the Case Vault. A report window includes the object's best shots, and video clips from the Case Vault will appear for editing.

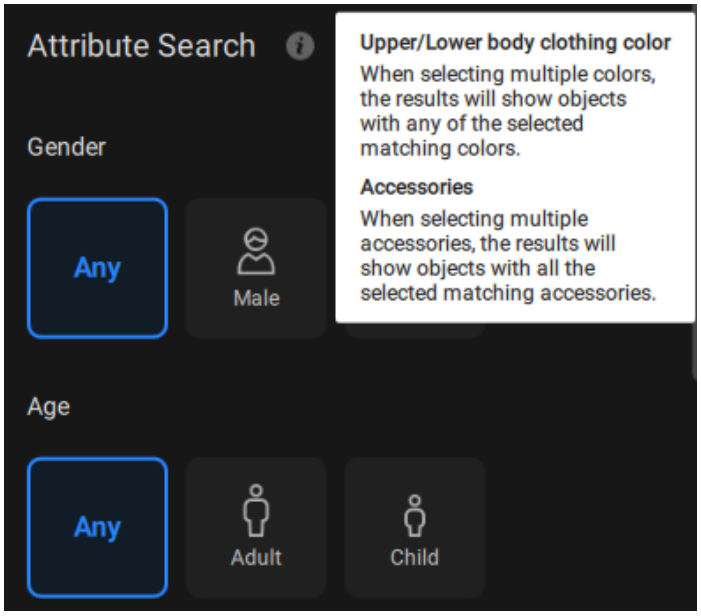
In the report's top right corner, click "Export" and choose to export the report as a PDF file or export all videos from the Case Vault.

IMPORTANT:

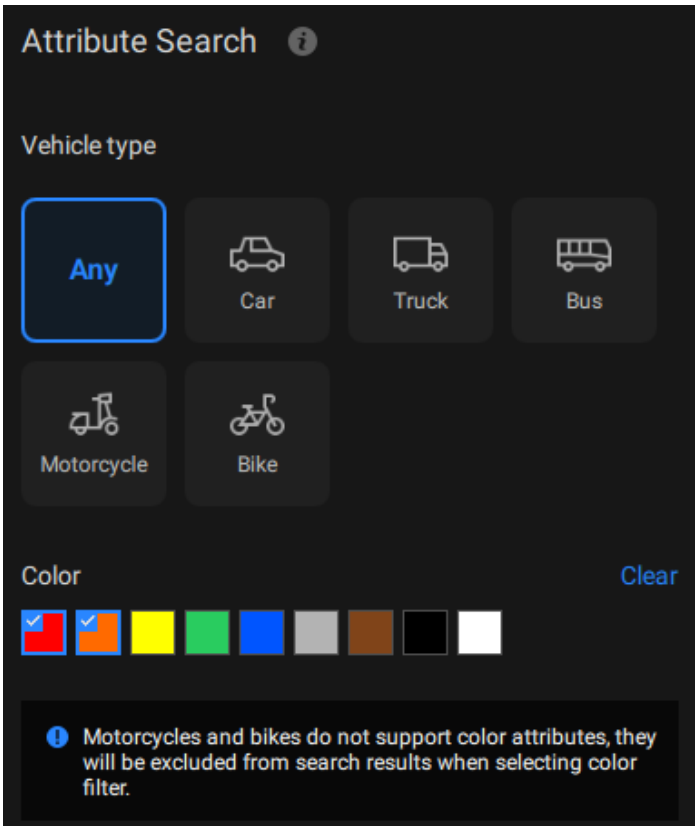
1. Starting from VSS v1.1, the object containing at least one selected color for the clothing or vehicle will be listed in the search results when one or more colors are selected in the clothing or vehicle color option. For full compatibility, it is recommended to upgrade both the client and servers/substations to the latest software/firmware version. For ND series NVR, please upgrade to 4.4 or later.



2. When searching for people with accessories, the search results will show people with both backpacks and hats.



3. When searching for motorcycles or bikes, color attributes are not supported.



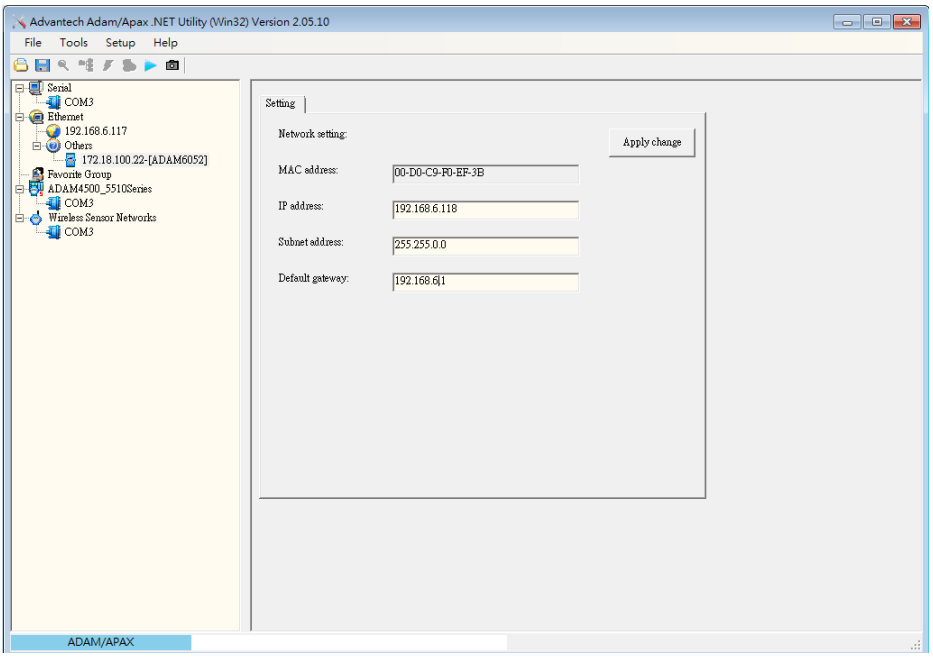
4. For Re-Search, a broader time frame and more selected cameras result in a longer search time. If the VSS server is busy checking and calculating a significant amount of metadata, it may reach a 90-second timeout with no search results. To avoid this scenario, consider shortening the time frame and reducing the selected camera count, and keep in mind that CPU and storage throughput will also influence the search speed.
5. The snapshots and metadata of Deep Search are stored in the same path as recordings and recycled based on the recording recycle setting. An object can generate approximately 0.25 MB of data. For mid-to-high activity scenes, such as parking lots, with about 10 objects per minute, the data capacity can take up approximately 150 MB of storage space per hour per camera.
6. To comply with regional privacy laws, the Deep Search function can be managed by users with an admin account in Settings > Preferences > Station > Deep Search. More details can be found in Chapter 4.
7. Please refer to the VIVOTEK'S website and check supported cameras for Deep Search. (https://www.vivotek.com/ai-driven/deep-search-system-requirement)
8. With a newly added camera, Deep Search takes 3 to 5 minutes to acquire search data. The searched results will be acquired after another 2 to 3 minutes.

Chapter 3: Applications

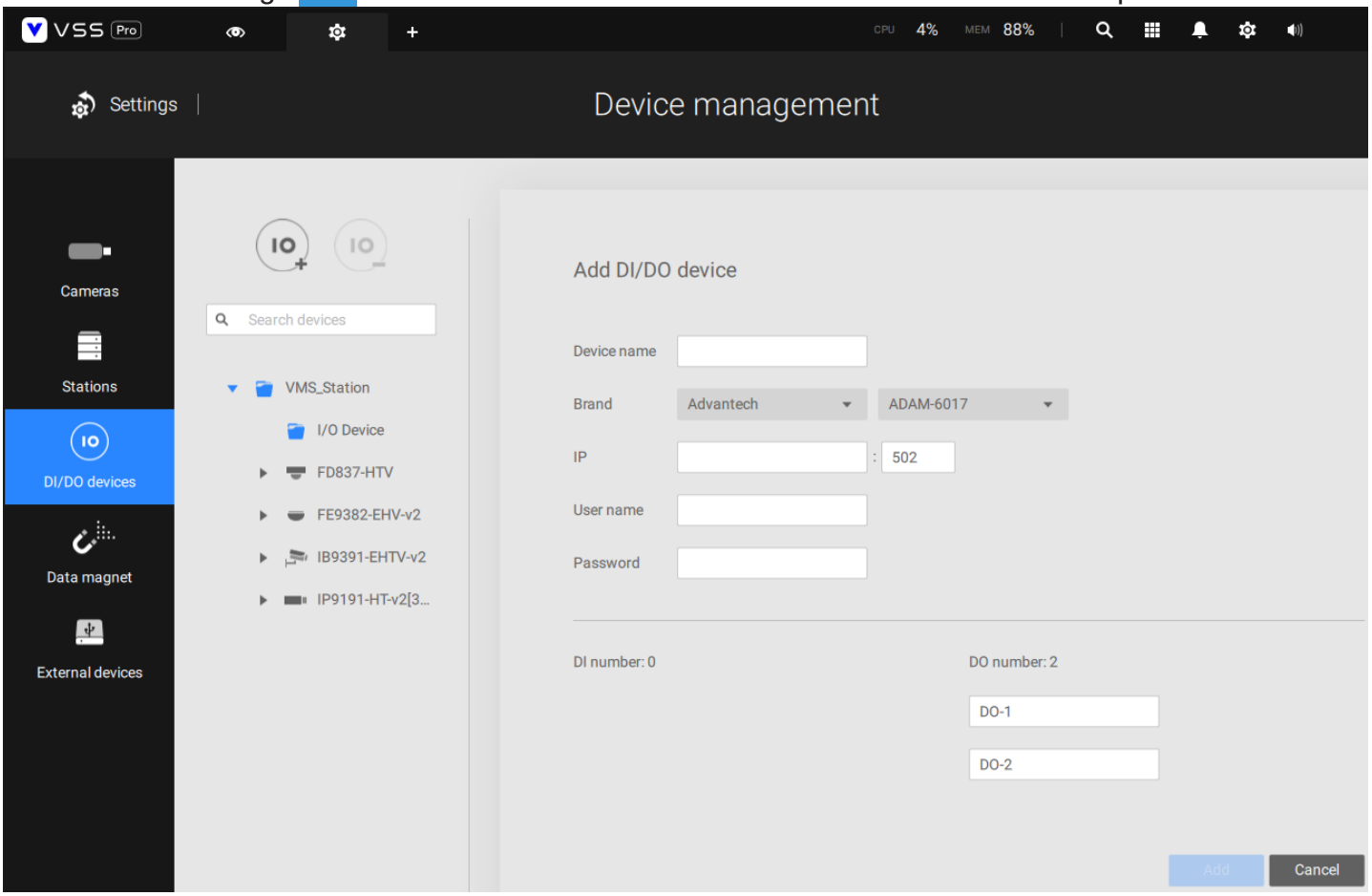
3-1. I/O DI/DO Devices

IO Box and Related Configuration

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



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

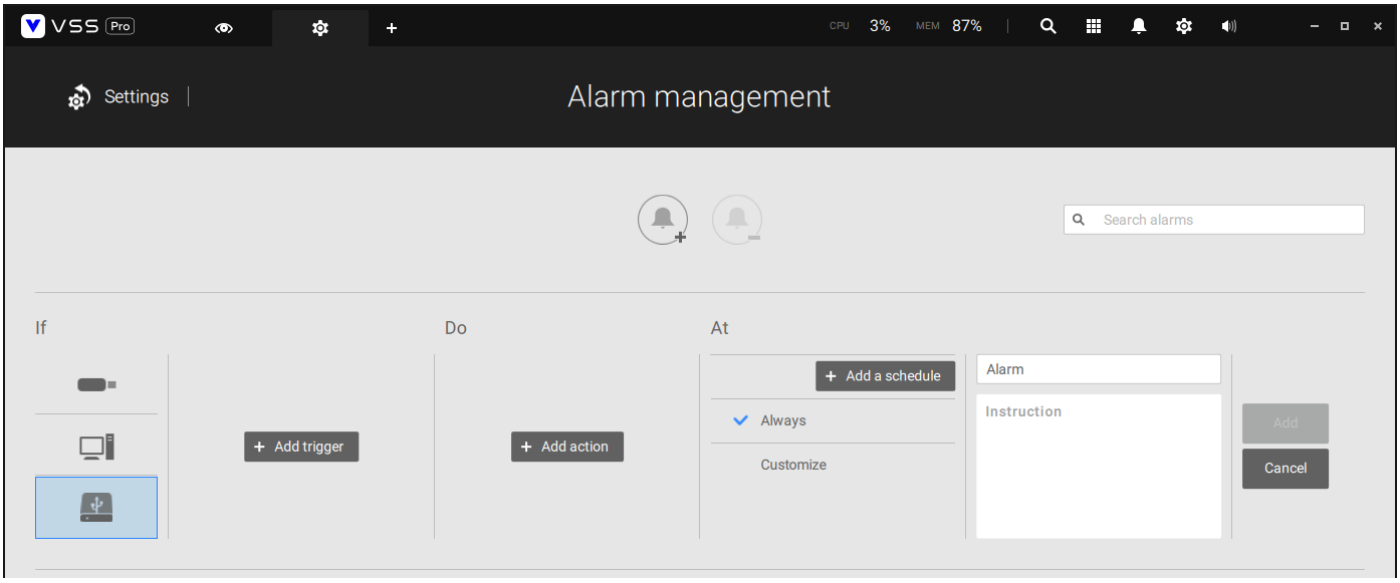


Enter the I/O box's IP address and credentials, and select the correct model name from the pull-down list on the right. Click the Apply button to proceed. The current I/O connections are also displayed on screen, such that the status is displayed when DI pins are connected to detection devices.

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** button + Add trigger.

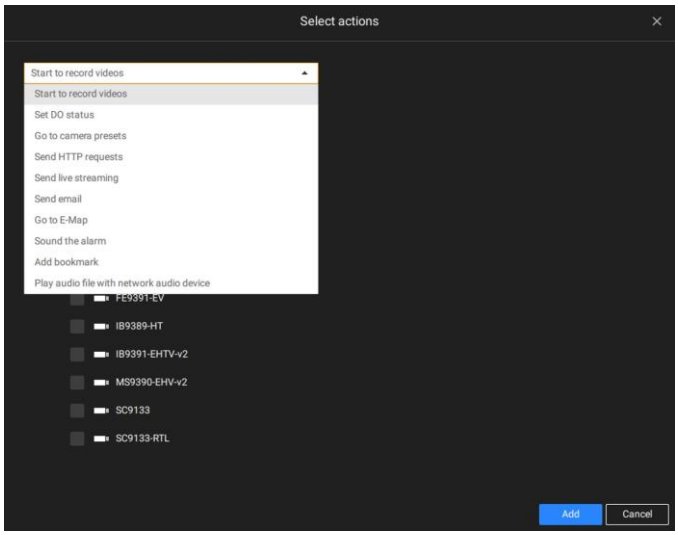


The **Select trigger and source** window will prompt.

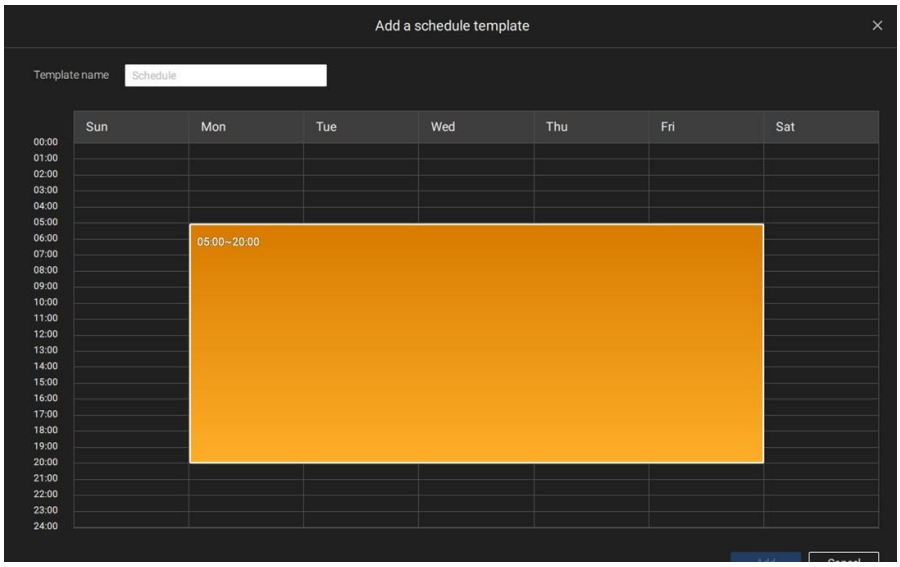
Select either the I/O Box DI or DO as the triggering source.

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

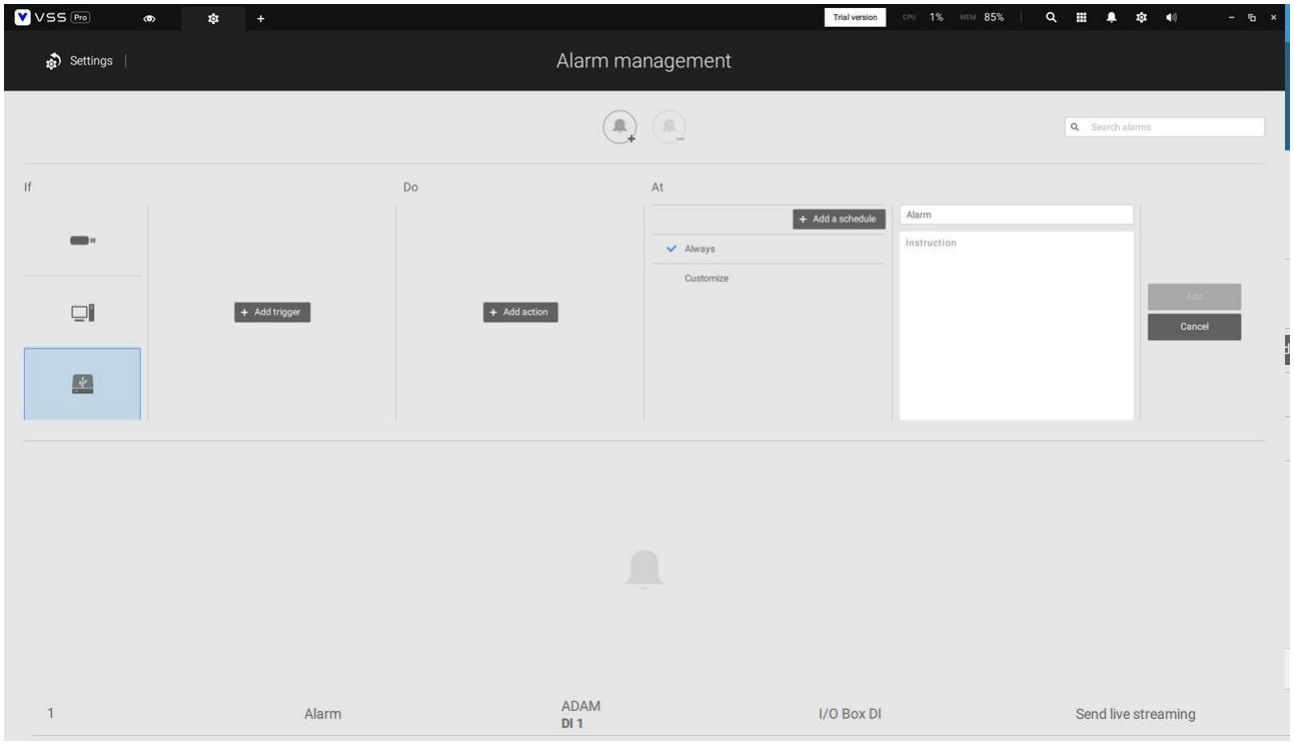
Click **Add action** + Add action, and select a corresponding action, such as sending live streaming, record videos, trigger a DO, sending an HTTP request, or sending an Email. When done, click the **Add** button.



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



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



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

3-2. Configuring Redundant Servers - Failover

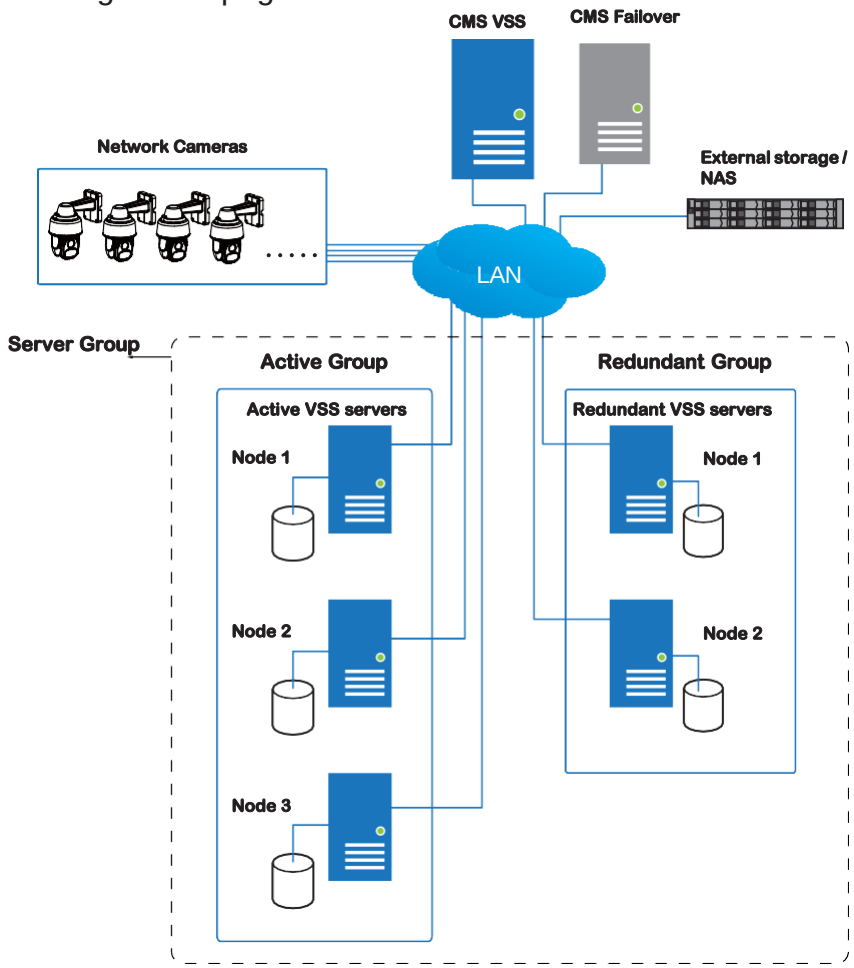
VSS servers can be configured into two groups: Active and Redundant. The Active group performs daily recording and monitoring tasks, while the Redundant group acts as the standby servers. In the event of server failures, the Redundant group becomes active, and takes over the recording task.

The Redundant server group configuration consists of the following:

1. One VSS server designated as the **CMS** (Central Management server) VSS central management server. Another VSS server can serve as a CMS failover server.
2. At least one VSS server in the **Active** group.
3. At least one VSS 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 VSS servers in the **Stations** configuration page before configuring the Redundant server groups. See the **Stations** configuration page.



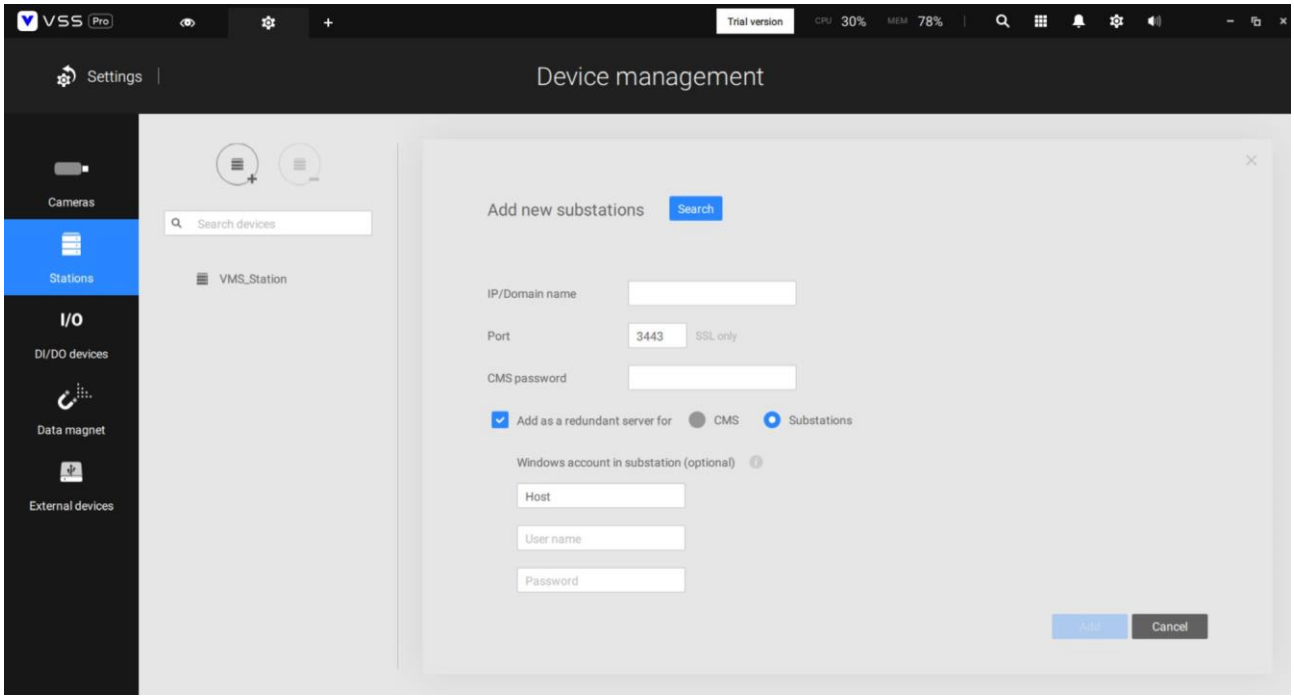
Below are the definitions of server roles:

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

1-1.	The CMS server is where the **Failover** configuration takes place.
1-2.	CMS continuously polls to check the heartbeats to monitor the statuses of all Active and Redundant servers.
1-3.	CMS backs up the configurations on active servers twice per day (8:00 am and 20:00 pm). Suggest manually applying the configuration while the license of active servers changes to prevent unexpected incidents occurring before daily backup.
1-4.	CMS assigns redundant server(s) to take over a failed Active server.
1-5.	In a Redundant server configuration, the CMS is supposed to be up and running at all times. If the CMS server fails, the server failover and failback operation will not take place. It is, therefore, preferable to configure a CMS redundant server and install the CMS server in 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** > **Device** > **Stations**. Click **Add Stations**, and select "**Add as a redundant server for**" "**CMS**." See the next section for the configuration procedure.

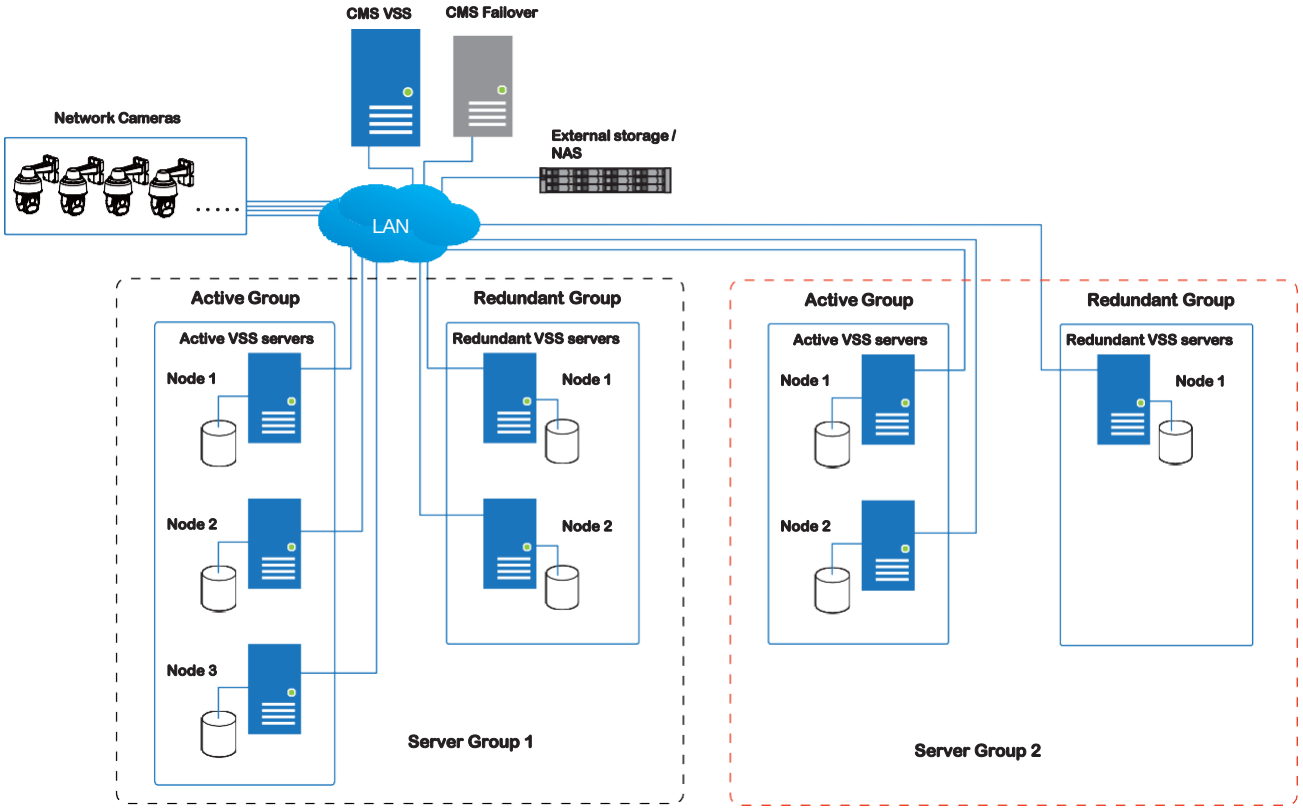


3. **Active** servers: Active VSS servers are the work horses that perform recording and monitoring tasks.
4. **Redundant** servers: The Redundant servers are actually active-standbys. They participate to continue video recording in the event of active server failures. It is recommended for the Redundant 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.

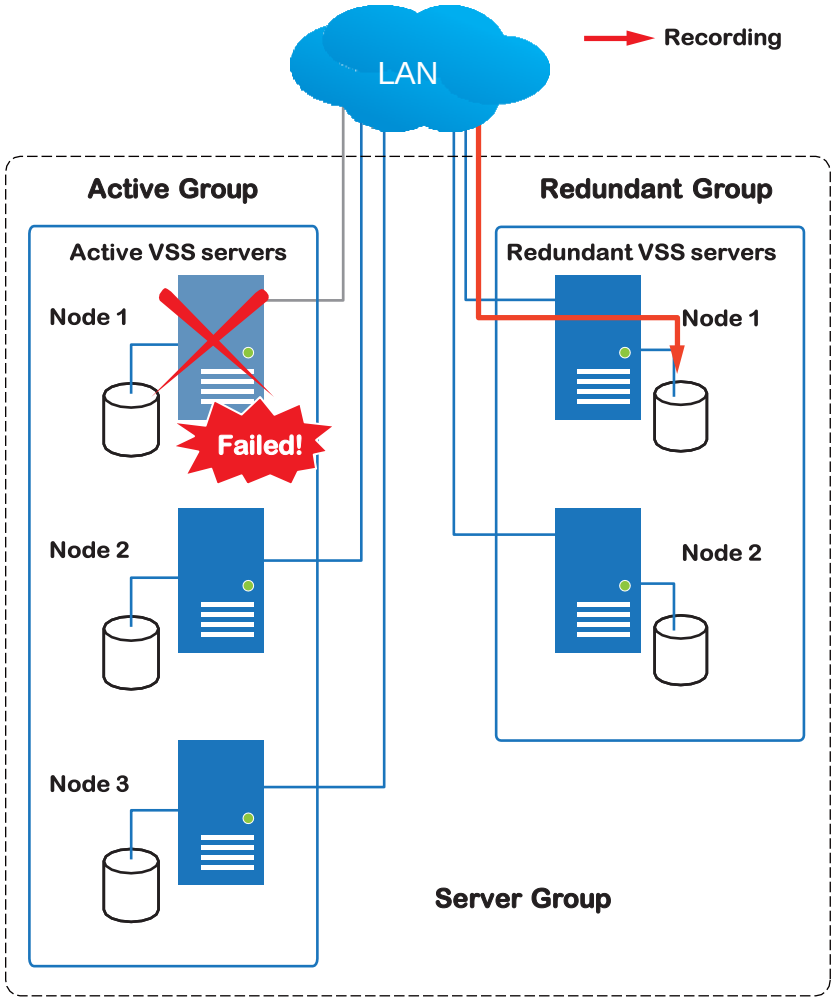
The conditions during the failover process are illustrated below:

Multiple Active and Redundant groups can be created.

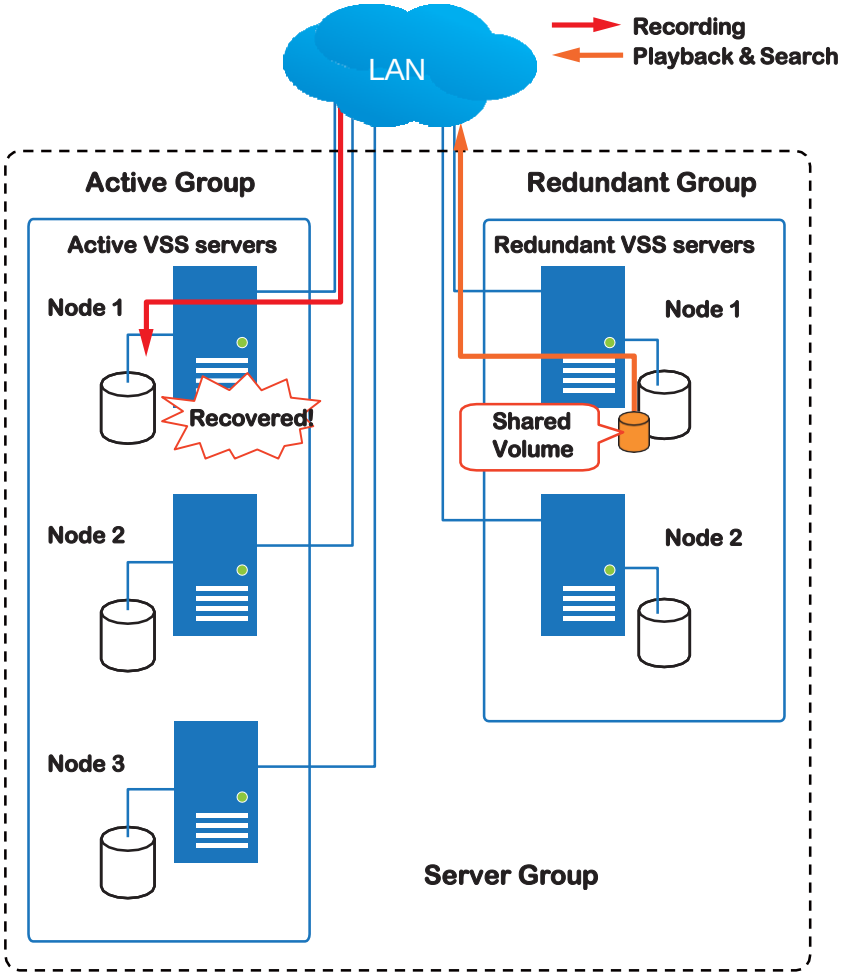


Each Redundant server can serve as the backup for ONE Active server. Depending on the number of the Active and Redundant servers, if the number of failed servers exceeds the number of Redundant servers, the failover will be abandoned. For example, if 2 Active servers failed, and there is only 1 Redundant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

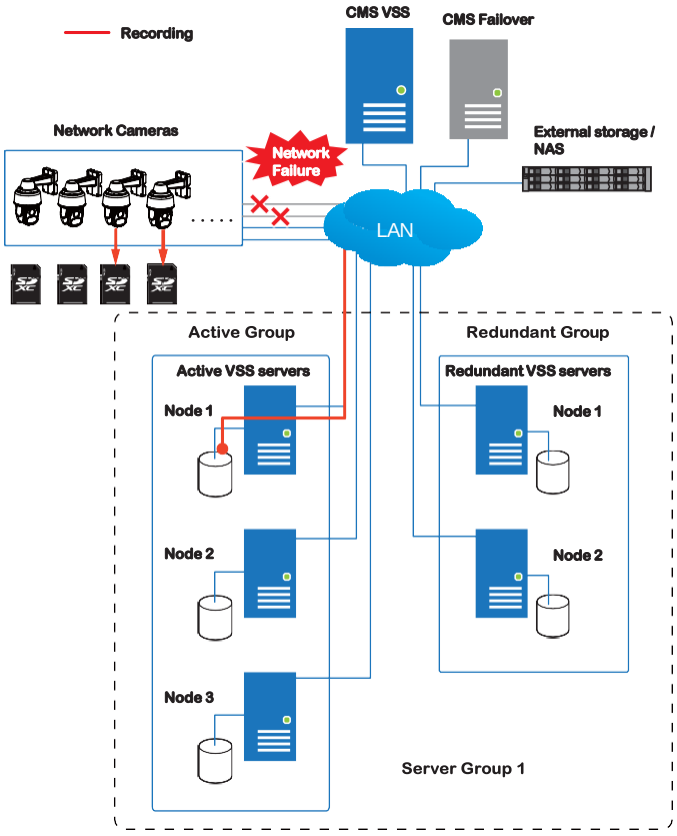
In the event of a server failover, a VSS server in the Redundant group takes over the recording task. Note that depending on the network environment, the takeover can take up to 5 minutes.



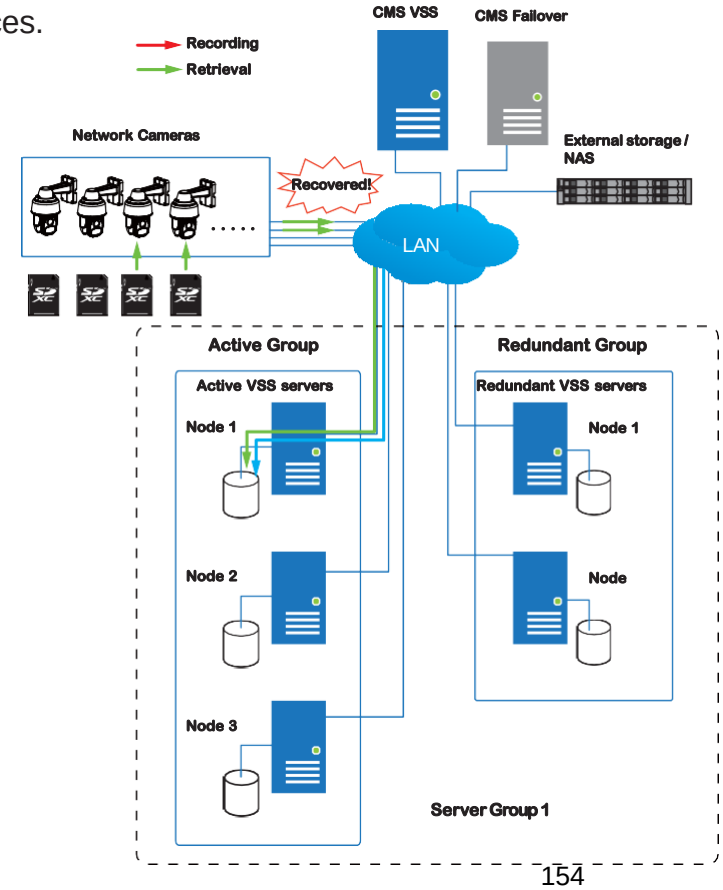
Once the server in the Active group is restored to normal operation, and a CMS server request for the recordings and data occurred during the time the active server failed, the requests will be fulfilled by a shared volume on the redundant server. Due to the concerns with network bandwidth and processing 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 VSS 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.



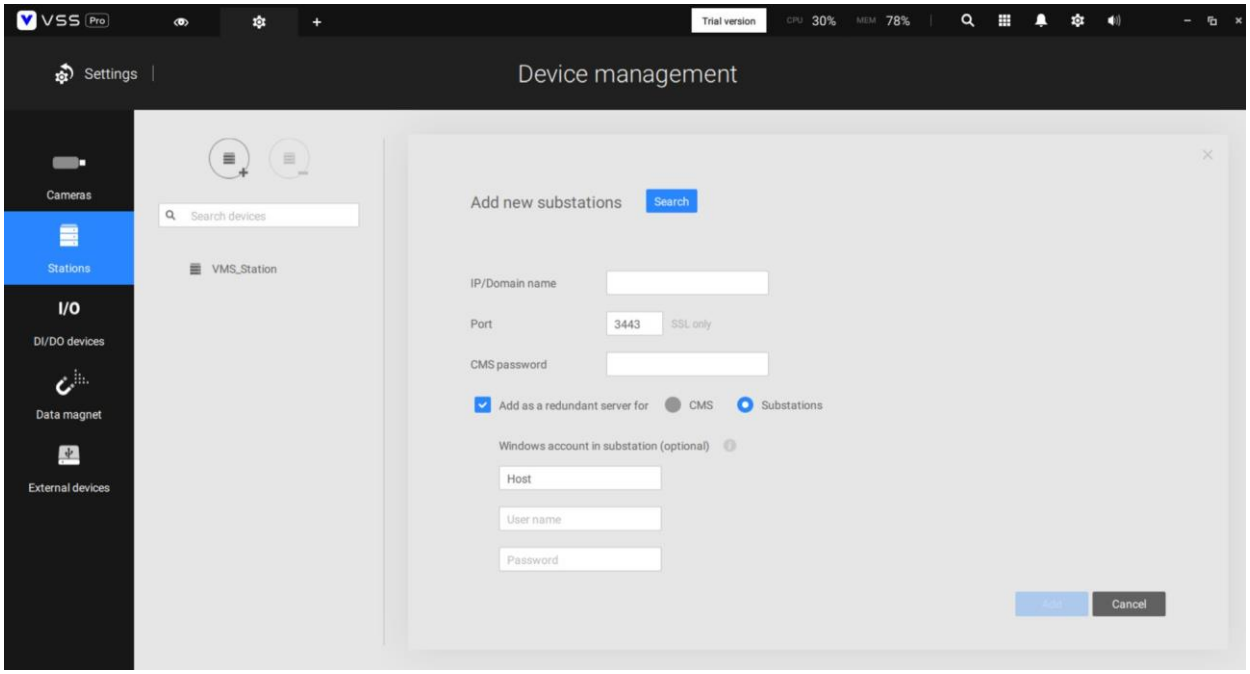
Once the network connection is restored, the VSS servers resume the recording task and also retrieve video segments from the SD cards. The video segments recorded during the network failure will be stitched up with those occurred before and after the network failure. The retrieval speed varies depending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



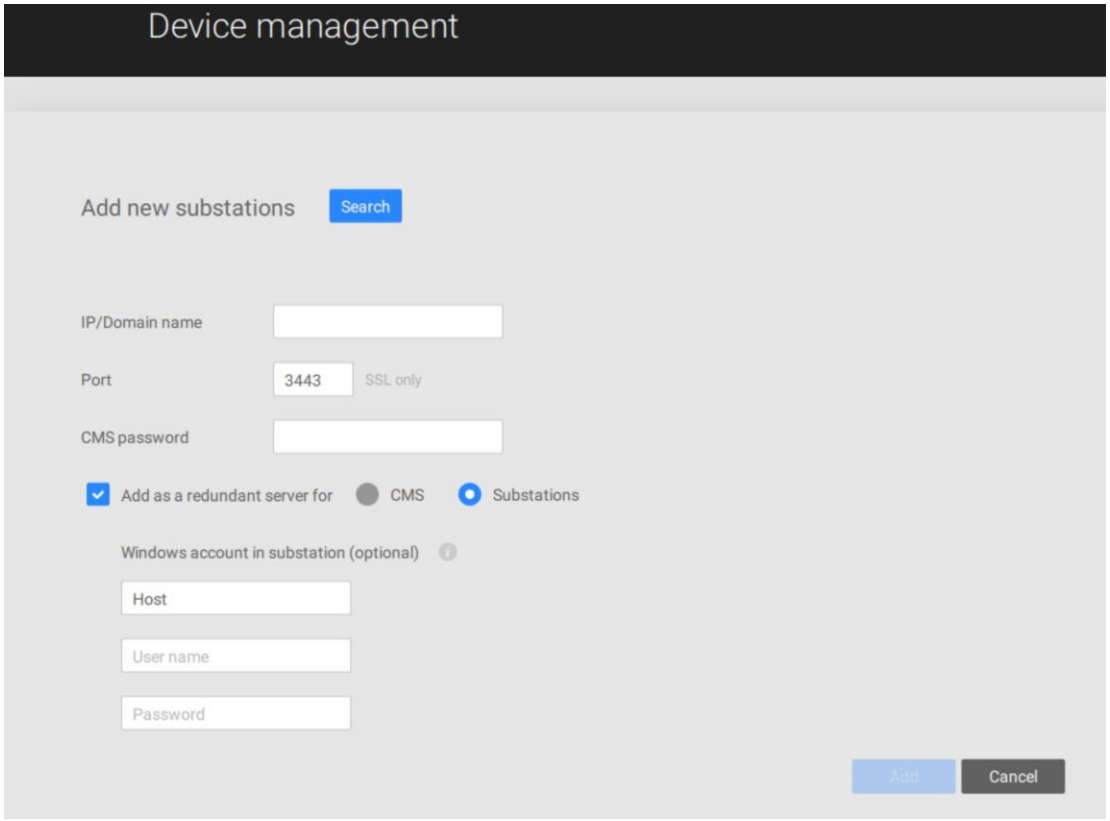
Failover Configuration Process

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

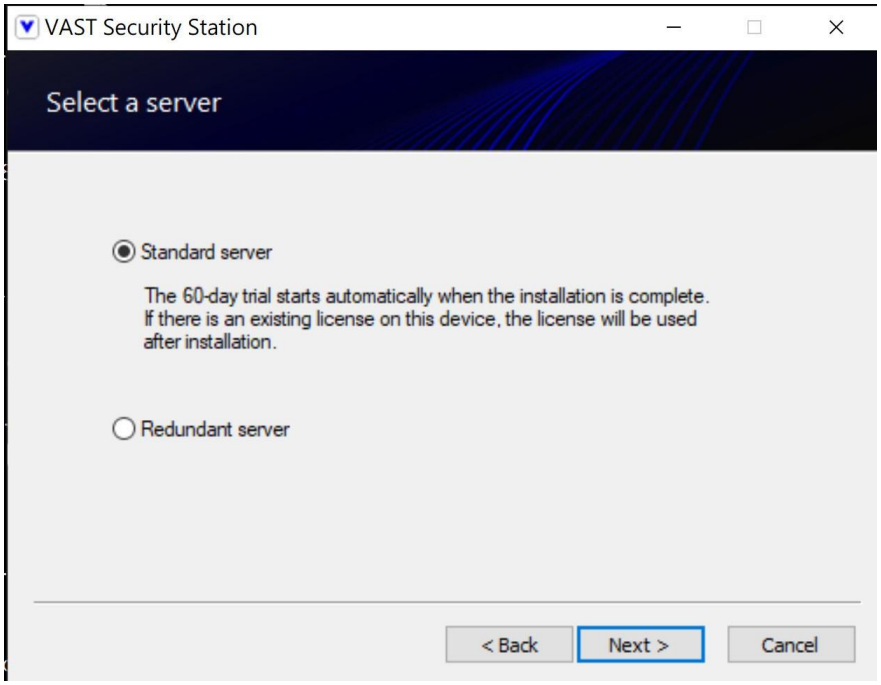
- If you are adding a Redundant server, select the "**Add as a redundant server**" checkbox, for either a **CMS** server or VSS **Substations**.
- If you are adding a server without selecting this checkbox, it will be considered as an **Active** server.
- When adding a Redundant server, you can provide 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.



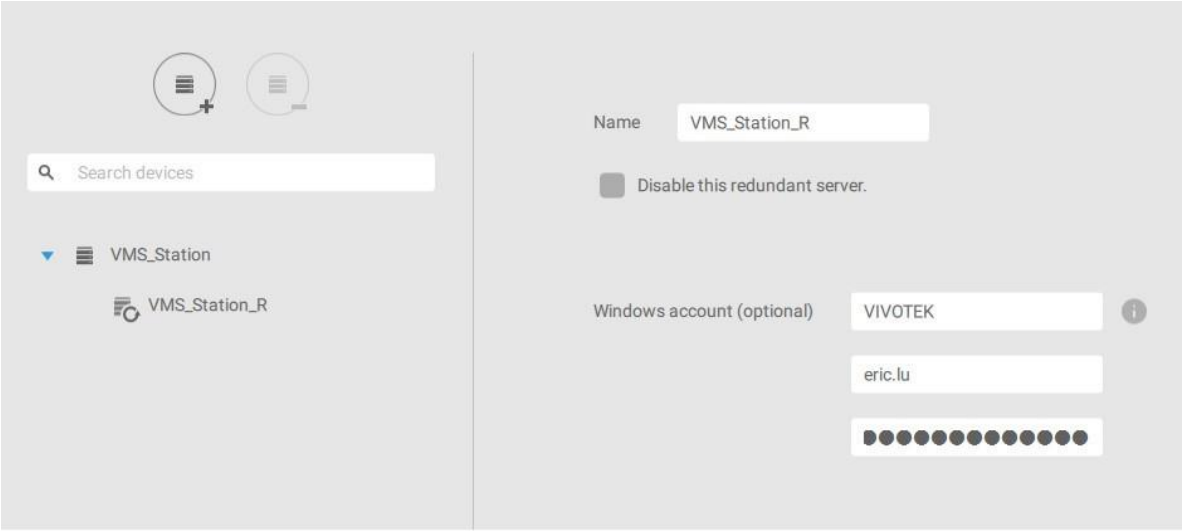
When the "**Add as a redundant server**" checkbox is selected, enter the name of your Windows domain and the user credentials for a full access to the Redundant server.



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



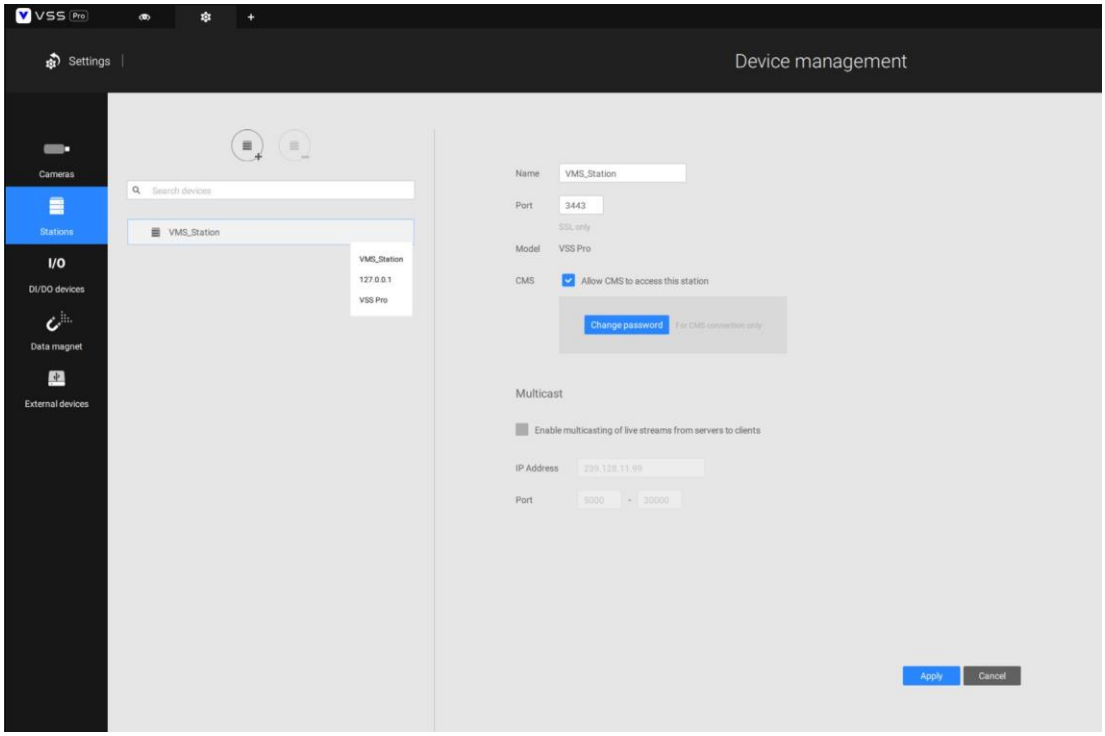
When a Redundant server is successfully added, the server will be listed under your VMS station.



A Redundant server comes with an associated icon, .

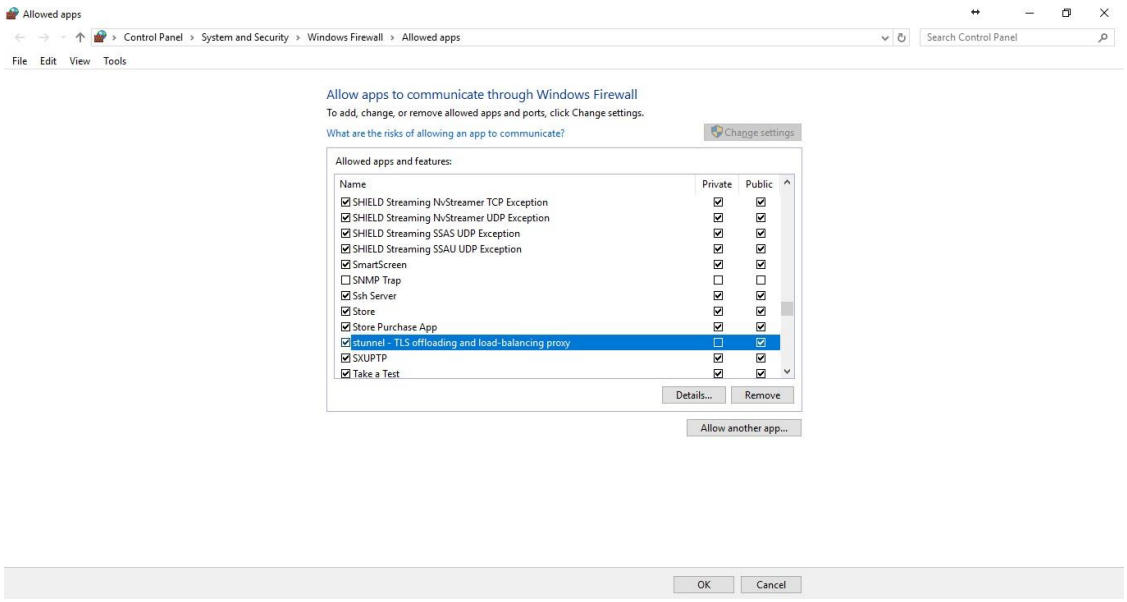
An Active server must have a CMS password configured for the hierarchical configuration.

Note that on the **Active servers**, you should configure them as the subordinates to your CMS VSS 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.



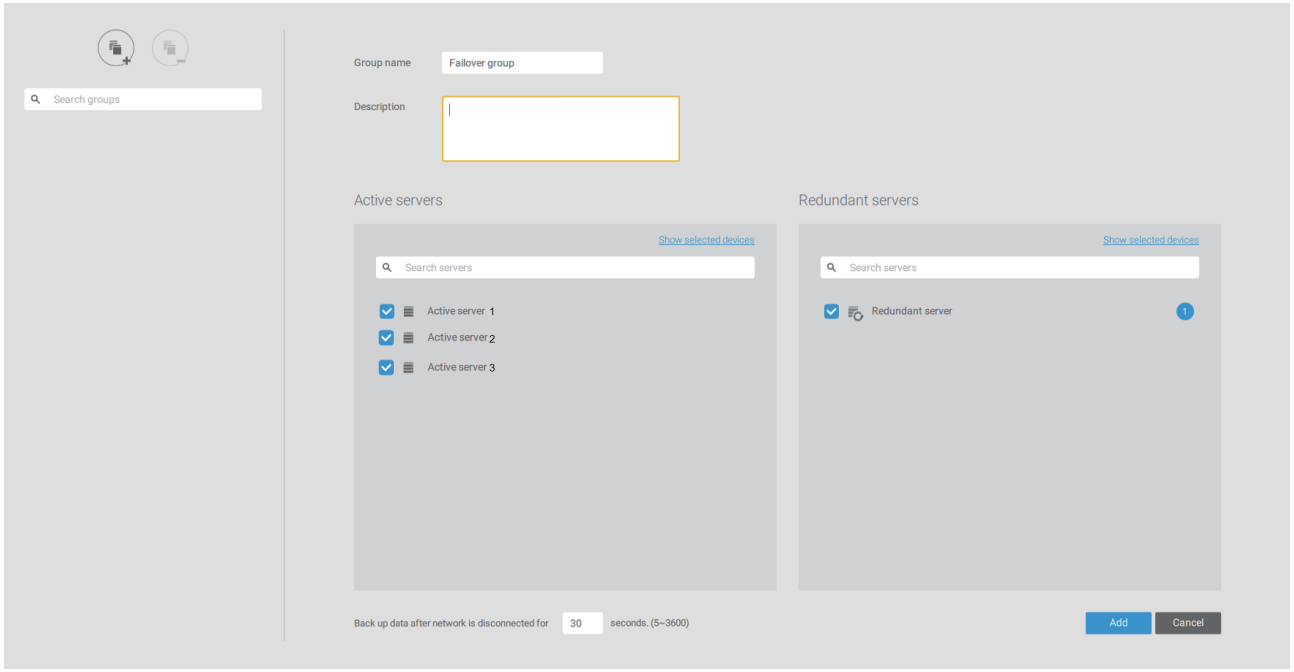
Two agents will be running on the Active and Redundant servers, "stunnel" and "VMSWebServer." Make sure they are not blocked out by your firewall. These agents can be found in the default folders below:

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

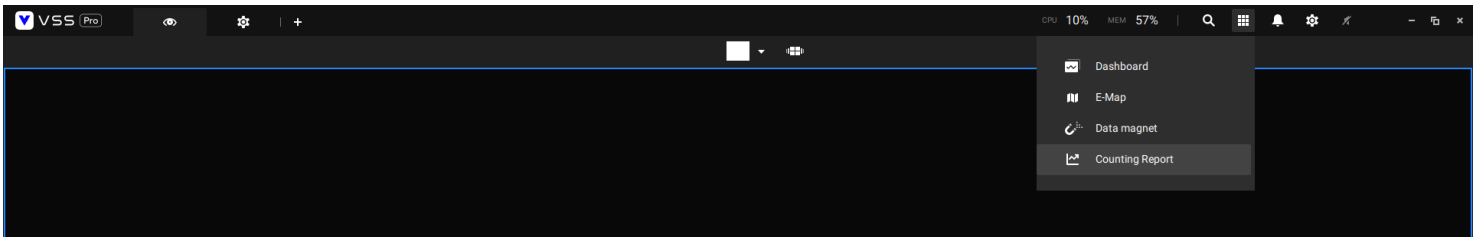


Click on the Add button to create a Redundant server group. The Active and Redundant servers you enlisted on the Stations page should all be listed below. Select the members of the Redundant group, and click Add to complete.

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.



3-3. Counting Report



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

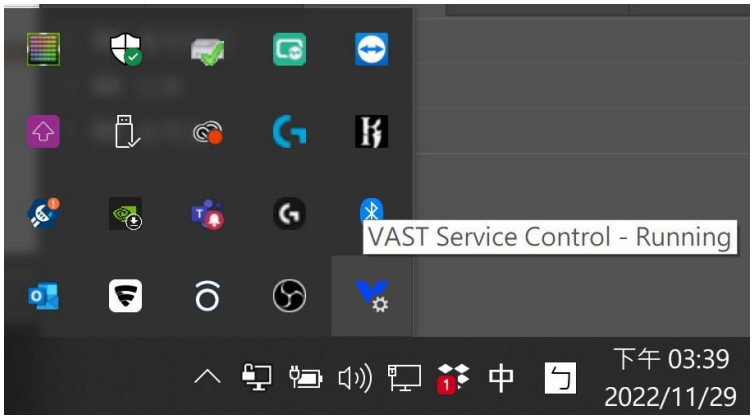
Note that the configuration of detection methods in People Counting still occurs on a web console to individual cameras. It is not configurable through the VSS LiveClient.

Prerequisites:

The prerequisites for using the Counting Report are:

1. The monitoring server running the Counting 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 VSS server instance runs in the background. The VSS management console does not need to be started during the Counting Report data collection process.

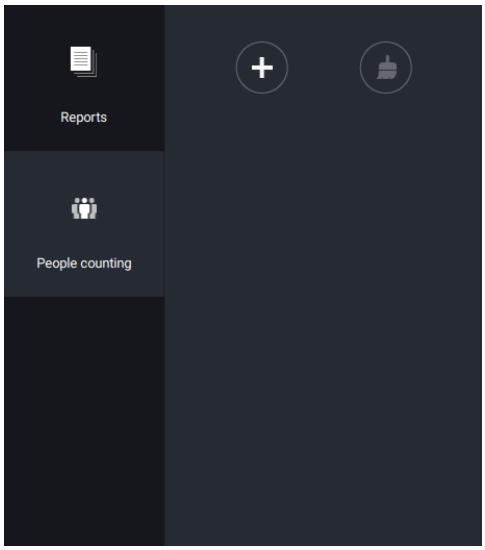


2. Cameras running the VCA utilities have been configured and added into the VSS deployment. The instances of available VCA rules will be listed in the **Area** panel.

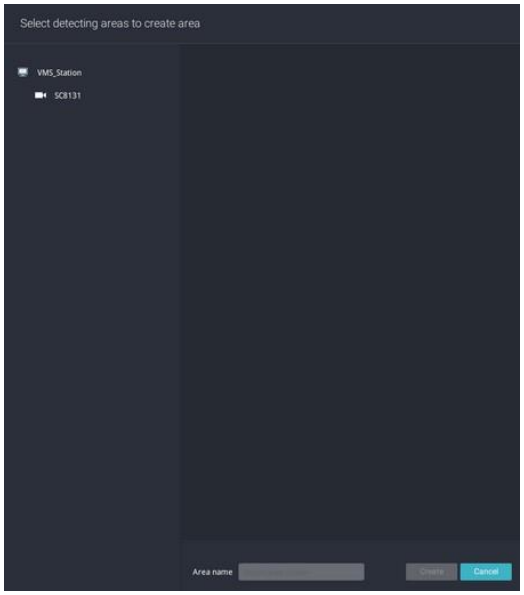
3. The life expectancy of VCA records is 5 years.
4. Currently the utility supports Windows XP, 7, 8, and 10.
5. The latest revision VSS supports Seamless Recording, in order to retrieve collected data and recording during Ethernet disconnection. Provided that an SD card is installed on the VCA-enabled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

To start Counting Report:

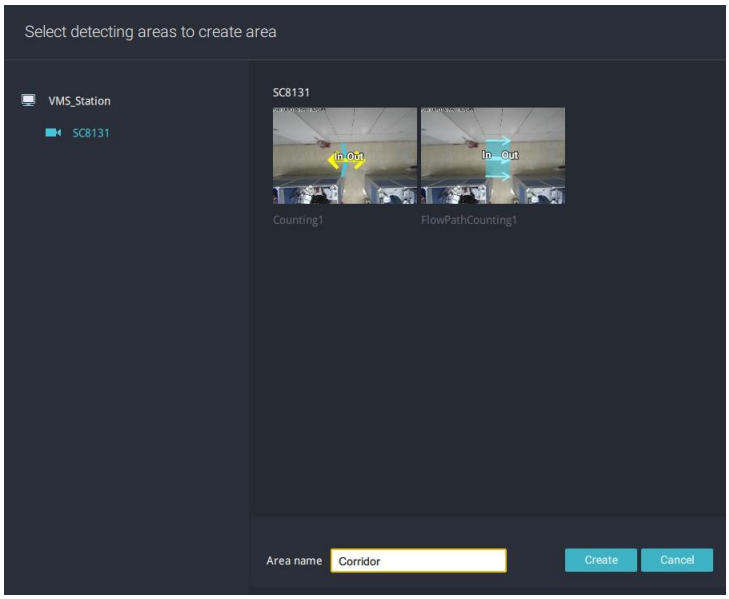
1. Click on Counting Report button on the tool bar.
2. Select People Counting.
3. Click on the Add area button.



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

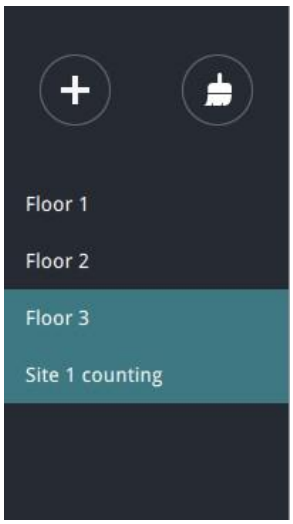


5. The pre-configured counting rules (areas) will automatically display. Select a counting rule and enter a name for the area. When done, click the Create button.



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

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



7. Select Date & Time

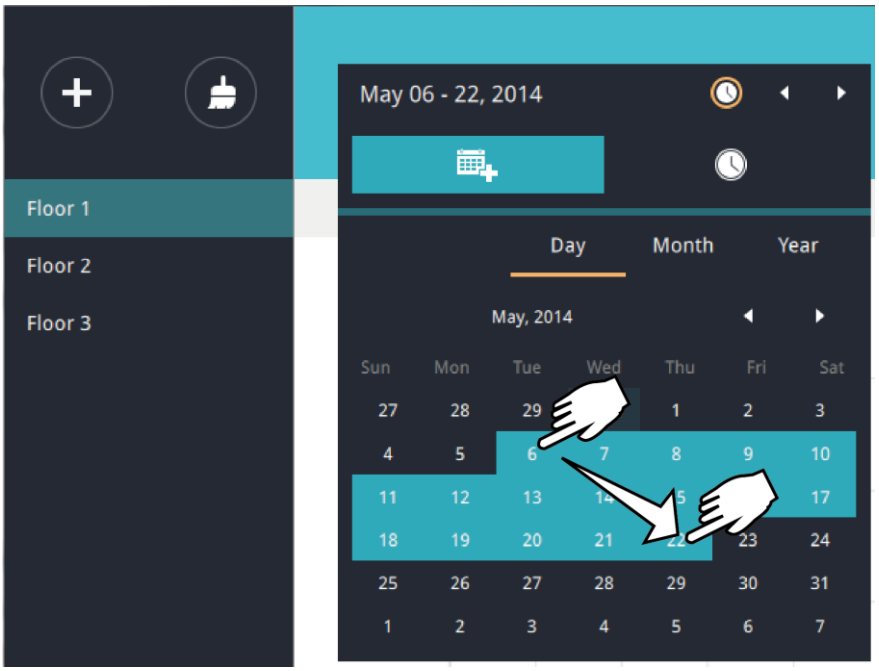
7-1. By default, the time displayed on the calendar is the current system time on the client computer running the utility. Select from the **Date** selector  on top.

7-2. Select a date or span of time from the calendar or use the **Time**  selector to select a span of time.

> Single-click to select a date or click and drag to select multiple dates.

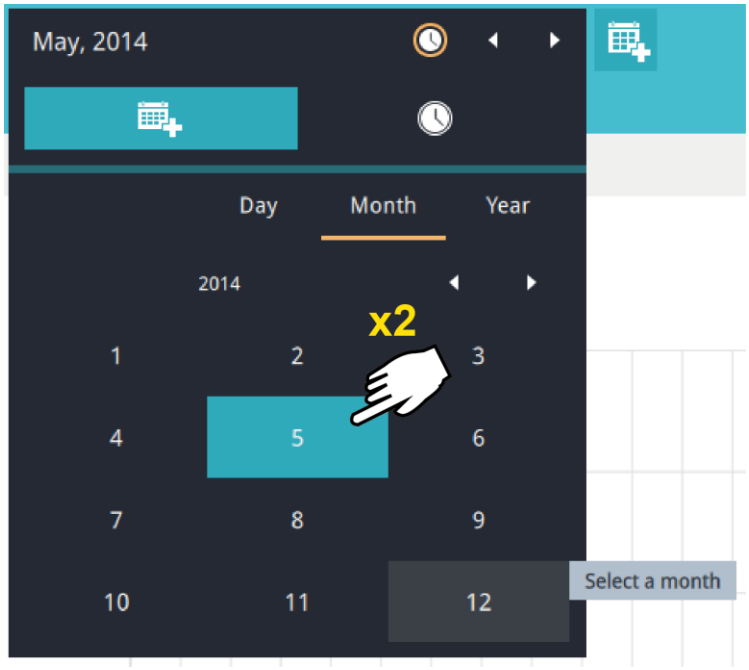
> You can select a month or a year using a single click. If you select a month, the timeline unit will be days within the month. If you select a year, the timeline units will be the months in a year.

> In the **Month** or **Year** panel, single click to select the entire month or an entire year. Double-click to select sub-units, e.g., days within a month. If you double-click on a Month panel, you will enter the Day panel.



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

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

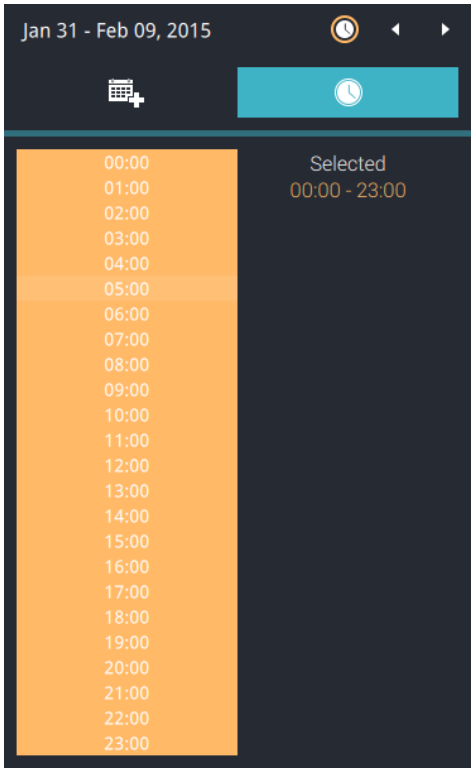


Note the following when making the configuration:

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

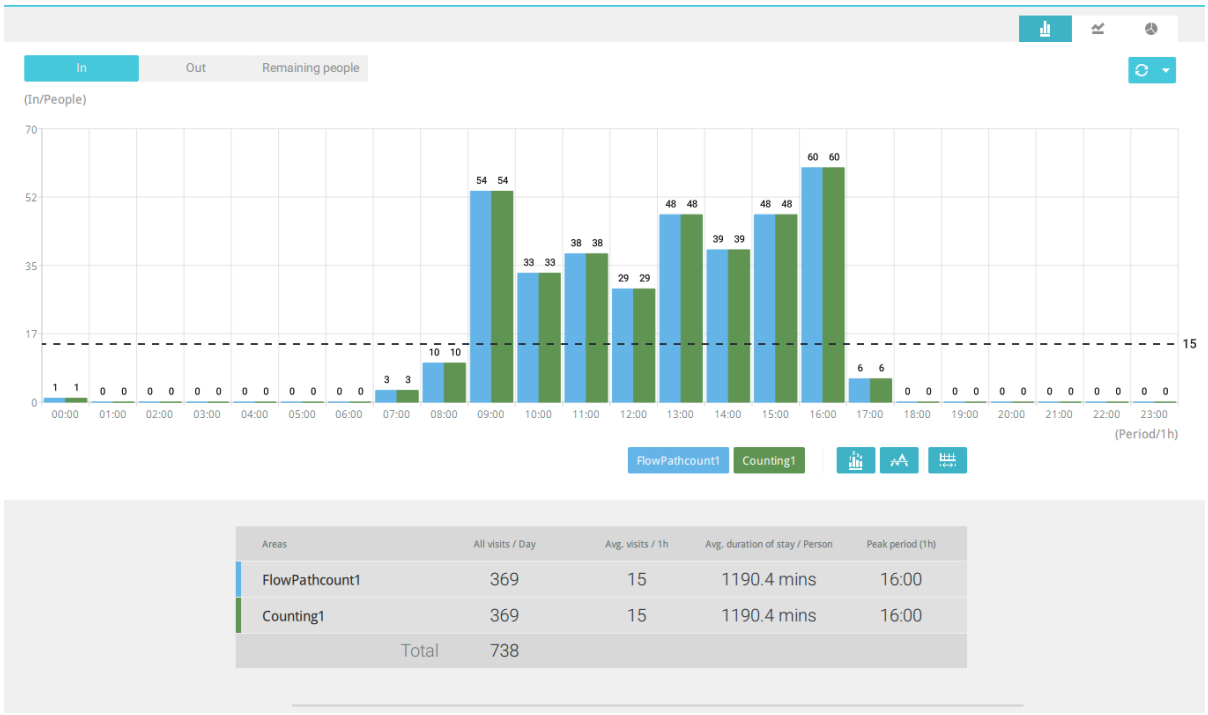
7-3. Select the hours to be included in the statistical poll using multiple clicks on the chart.

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



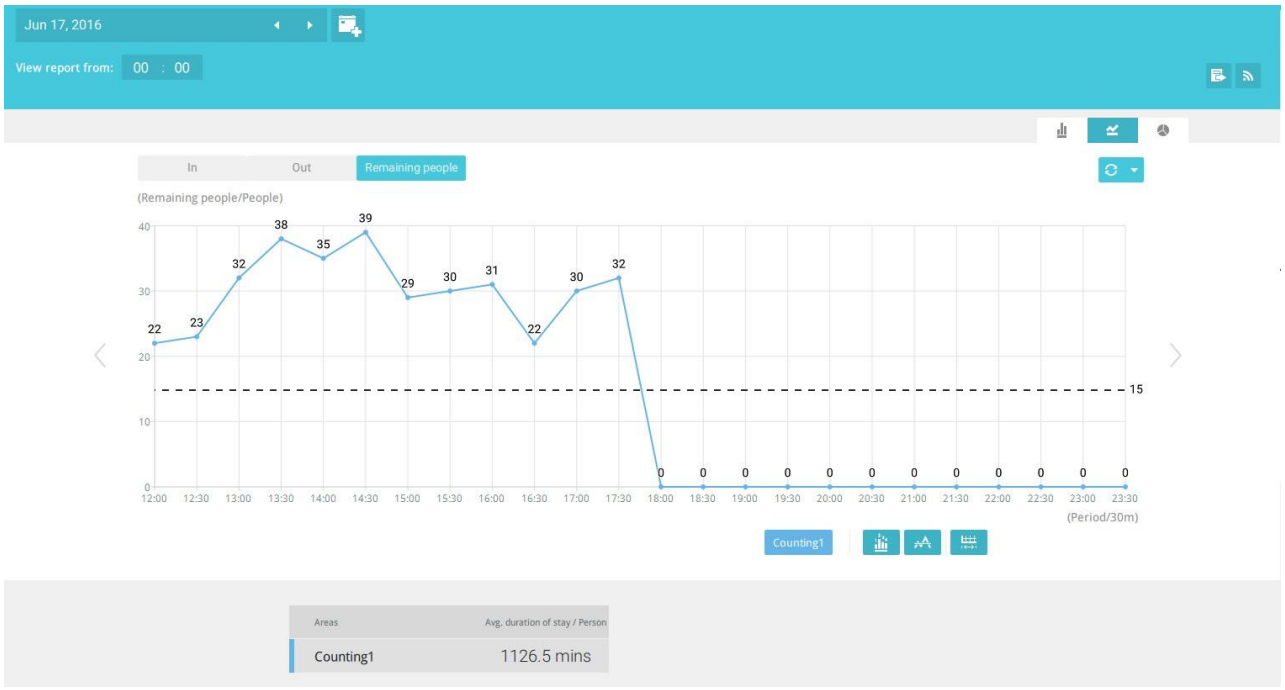
Note that you can only compare the counting results from two spans of time if you select only one Area. If you selected multiple Areas, you cannot compare the results from multiple time spans.

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

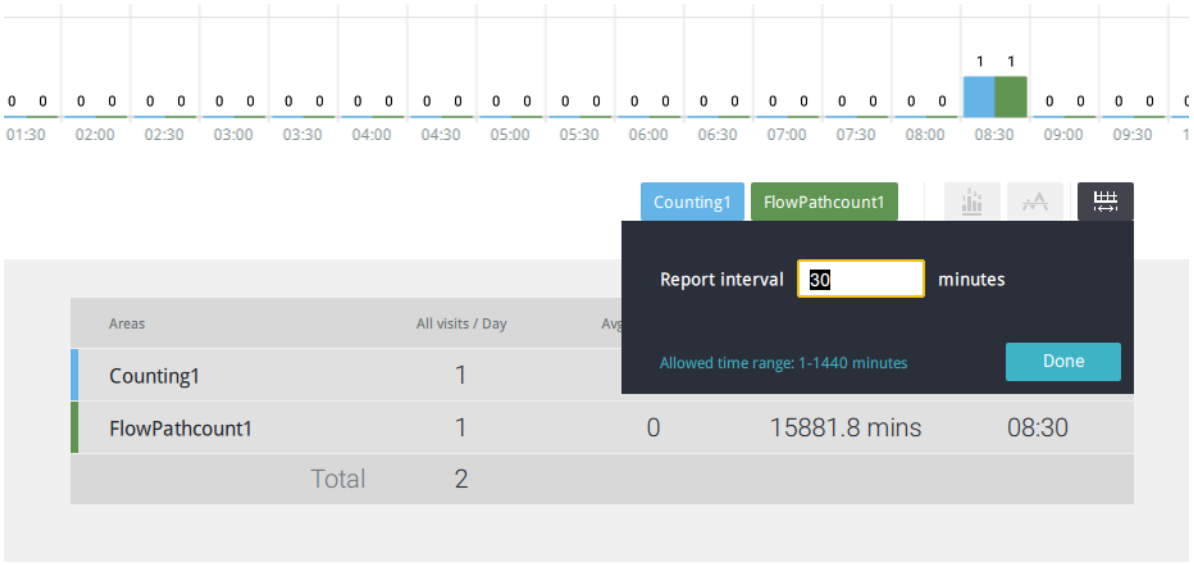
Note that the timeline units can vary depending on the span of time you selected on the Calendar panel. If a date was selected, hourly data will display in chart. If a year was selected, monthly data will display in chart.

Use the following functional buttons to change the display parameters.

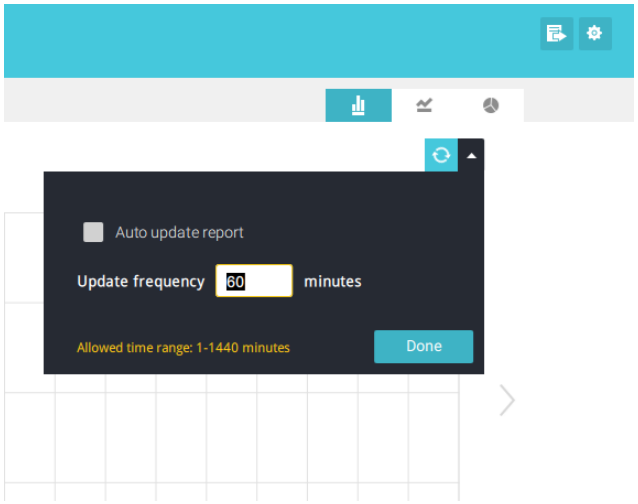
Show data on chart  : Displays the collected numbers on chart.

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 compared to the number acquired by every hour.

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



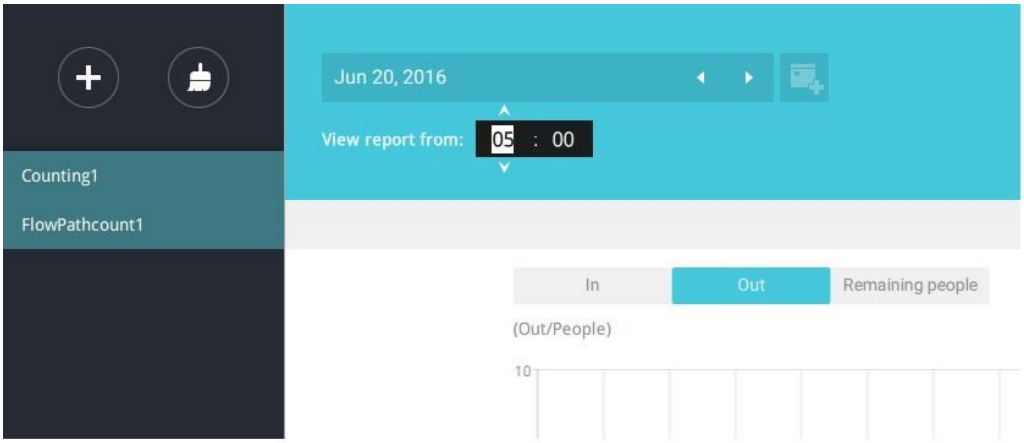
You can use the update menu on the side of the Refresh button to determine an automatic update schedule. You can let the statistic chart update itself by a regular interval.



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

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

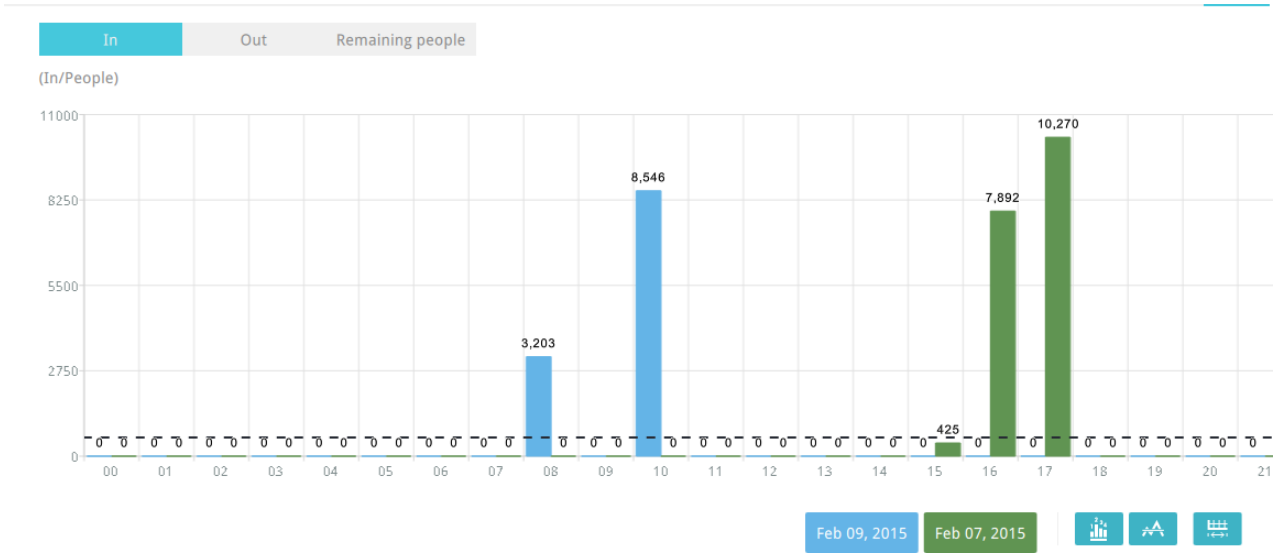
Use the time selector on the **View Report from** pane to select the start time of your statistics view window. Data collected before that time will not be displayed.



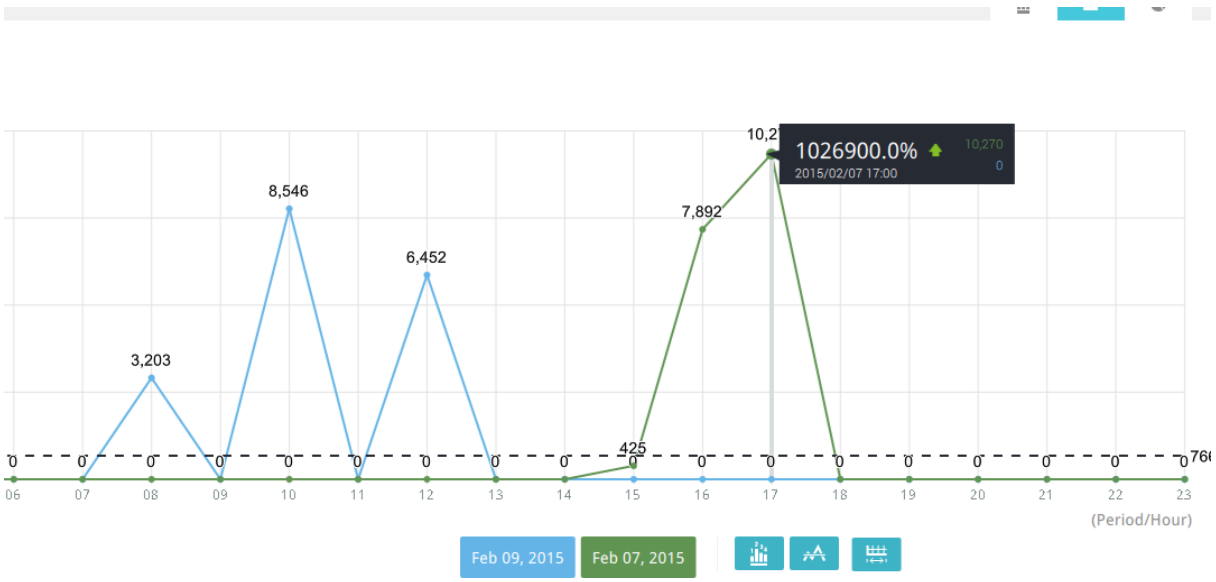
A number is displayed when you mouse over an area on the chart. Move your cursor to an area on chart, and the number is displayed.

Data on a timeline 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.

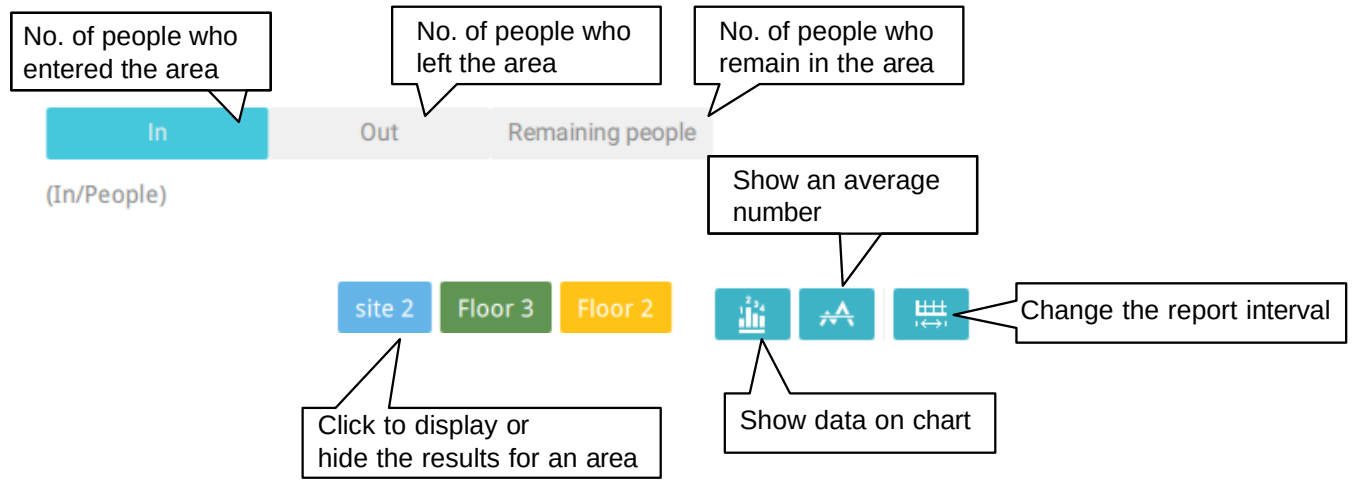
Note that the **Compare** function only applies when you select to display only one area on the screen.



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.



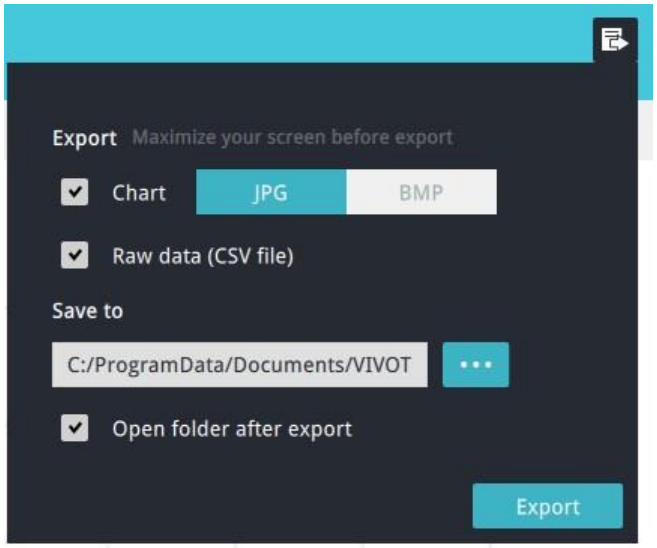
In addition to the charts, a summary of displayed data will be listed below showing the areas involved, visits/Day or Month, Average visits / Hours / Days, Average duration of stay / person, and the Peak hour.

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:\Users\Public\Documents\VIVOTEK Inc\VAST\Client\VCAReport

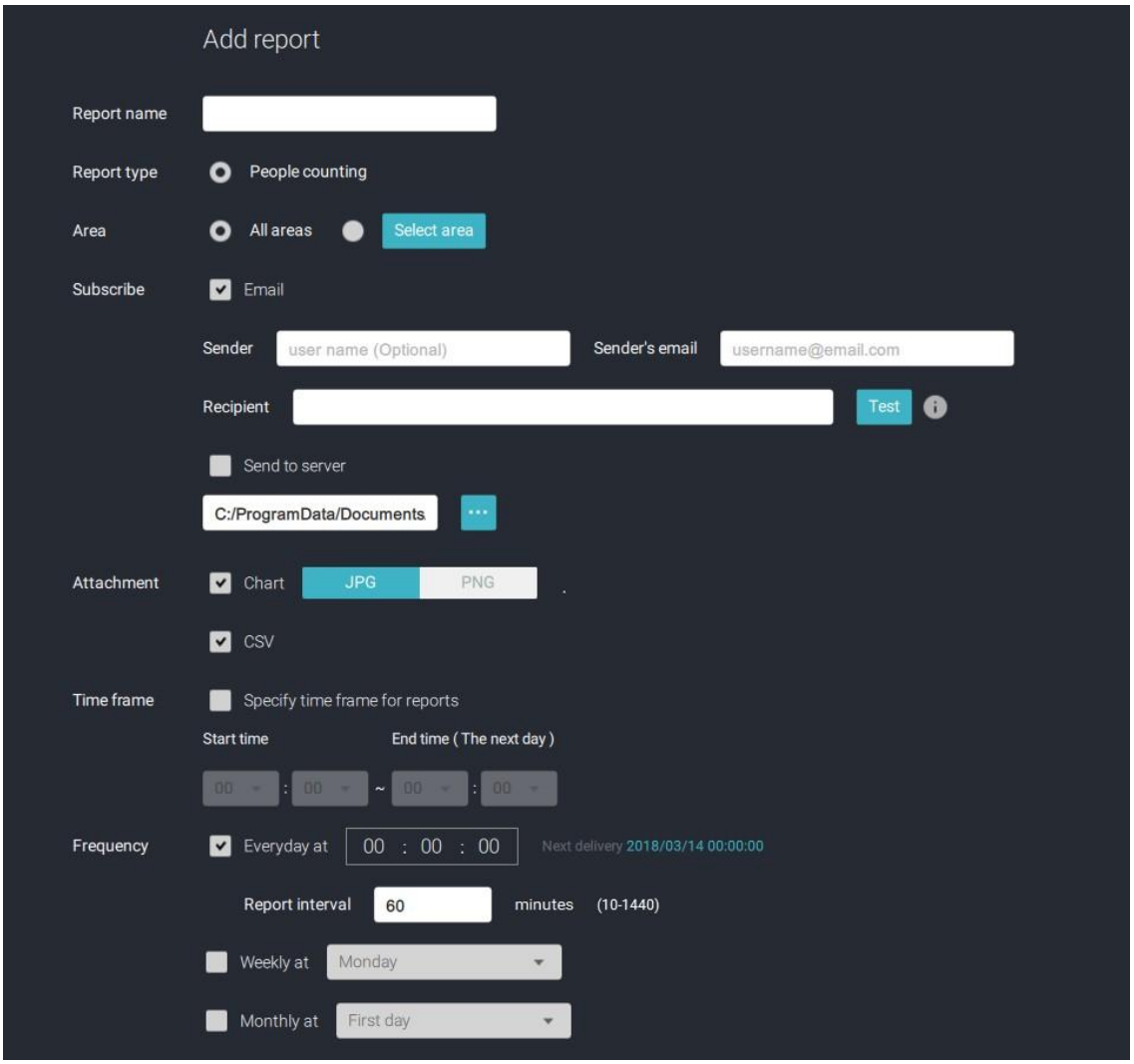


9. Click the Reports Subscription button to configure the regular report sent to your Email account or a specific location on the server itself.
   Select the following:

1.	Report type: People counting results, or Heatmap (Heatmap does not produce 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 VSS server. This VCA mail notification utilizes the mail service on VSS for regular notification. You can then receive Email notification every day on your Email account. You can enter up to 5 recipient addresses.

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



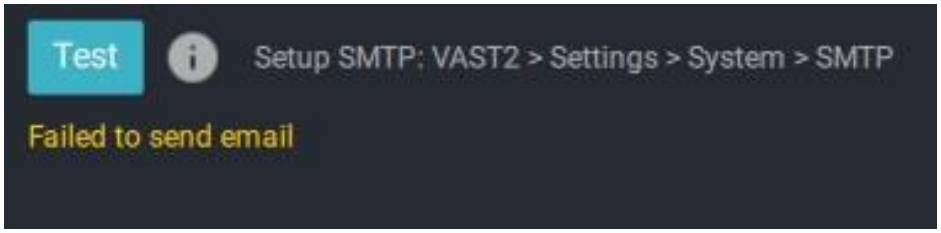
Note that the notification contents is your current field of view, including a Bar, Line, and Pie chart combined into one image file. The In/Out/Remaining results will be generated into 3 charts. Each Area will generate one CSV file, and each CSV data file will contain In/Out/Remaining/Summary information.

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

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

You may configure to receive regular Counting Report as Weekly or Monthly using the associated menus.

Below are the messages with the Email test function.



3-4. Data Magnet

What is Data Magnet?

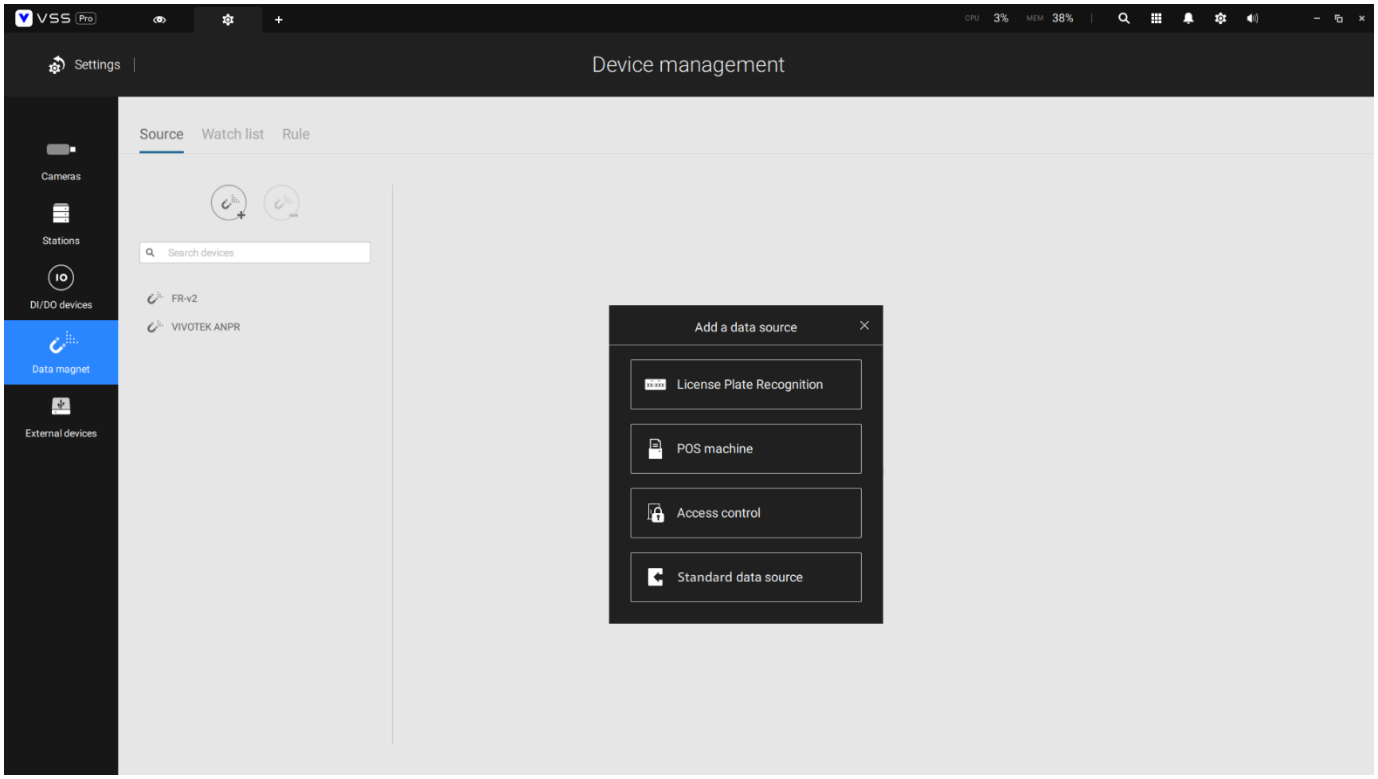
Data Magnet is an open platform for external hardware or software systems to integrate external data into VSS and VAST2, such as Access Control, License Plate Recognition (LPR), Barcode Scanner, etc.

Initial Setup

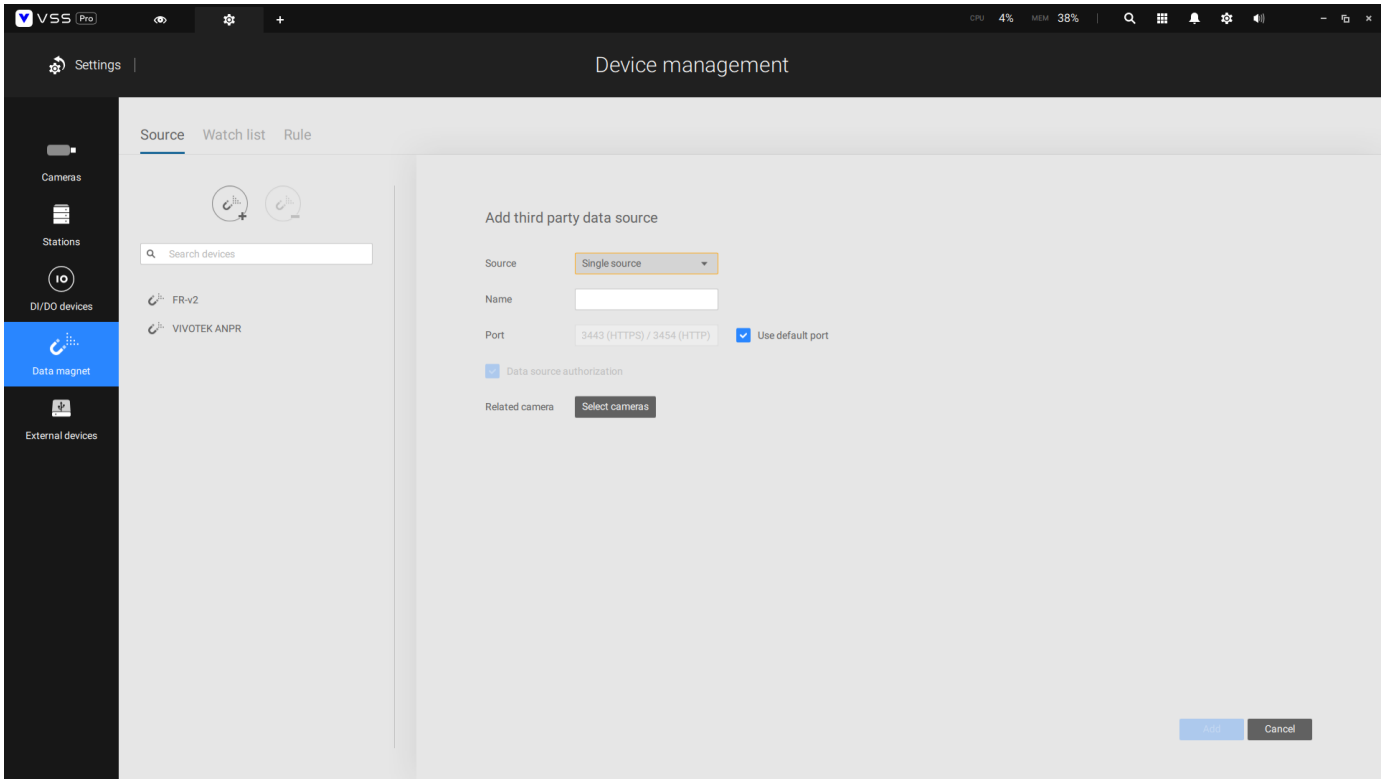
The first step of setup is to add a data source first. Data source refers to the external system that sends data to VSS.
Before setup, you can refer to the integration file of the data source you want to add.

Different external systems need to choose different data source types.

- Select Standard data source if the external system providers conform to the Data Magnet integration standard.
- Select License Plate Recognition for VIVOTEK LPR camera.
- Select Access control if the access control providers especially integrate with VSS.
- Select POS machine if the POS machine providers especially integrate with VSS.



After selecting the Data source type, you need to set the port to receive data from the data source. The port setting must be the same as the data magnet setting at the other end of the external system you want to receive. If Data source authorization is ticked, the data magnet on the external system side needs to enter the VSS login account and password to receive the data. The related camera is to choose which camera image is related to the incoming data.



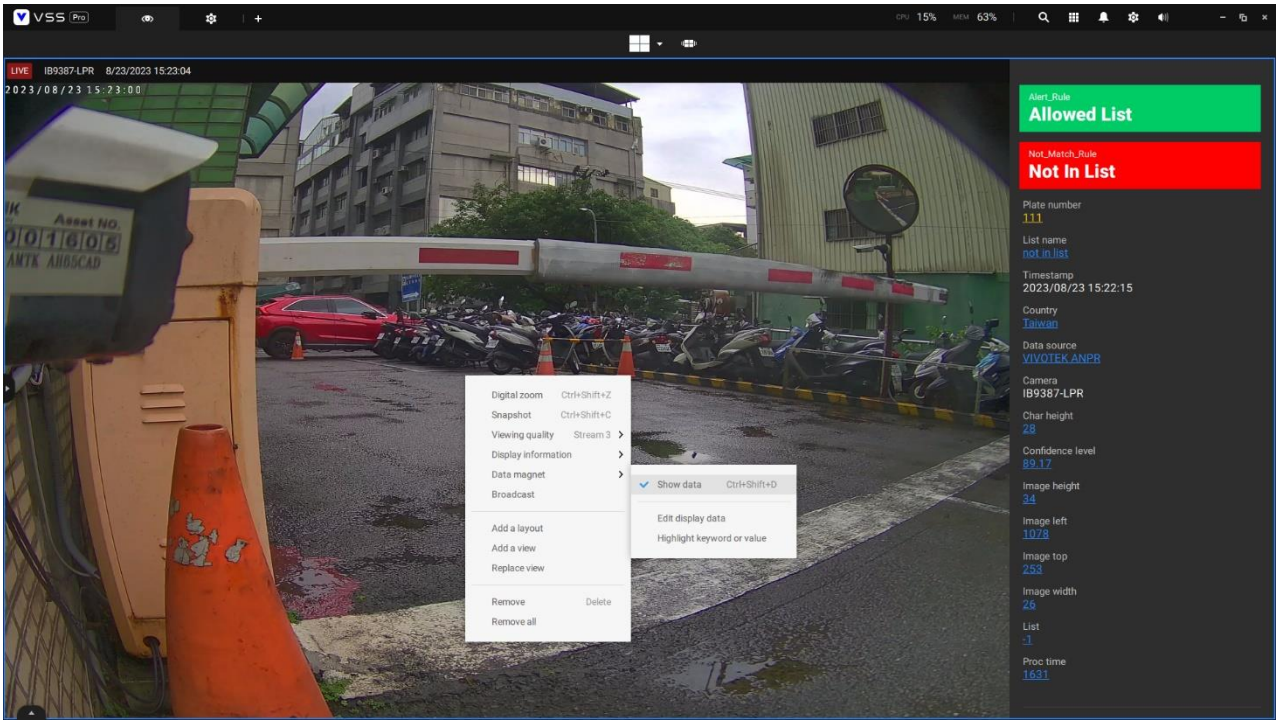
Data Magnet Function

After adding Data source, Data Magnet can use the following three main functions:

1. Live View Display Data
2. Watch List Trigger Actions
3. Data Magnet Search

Live View Display Data

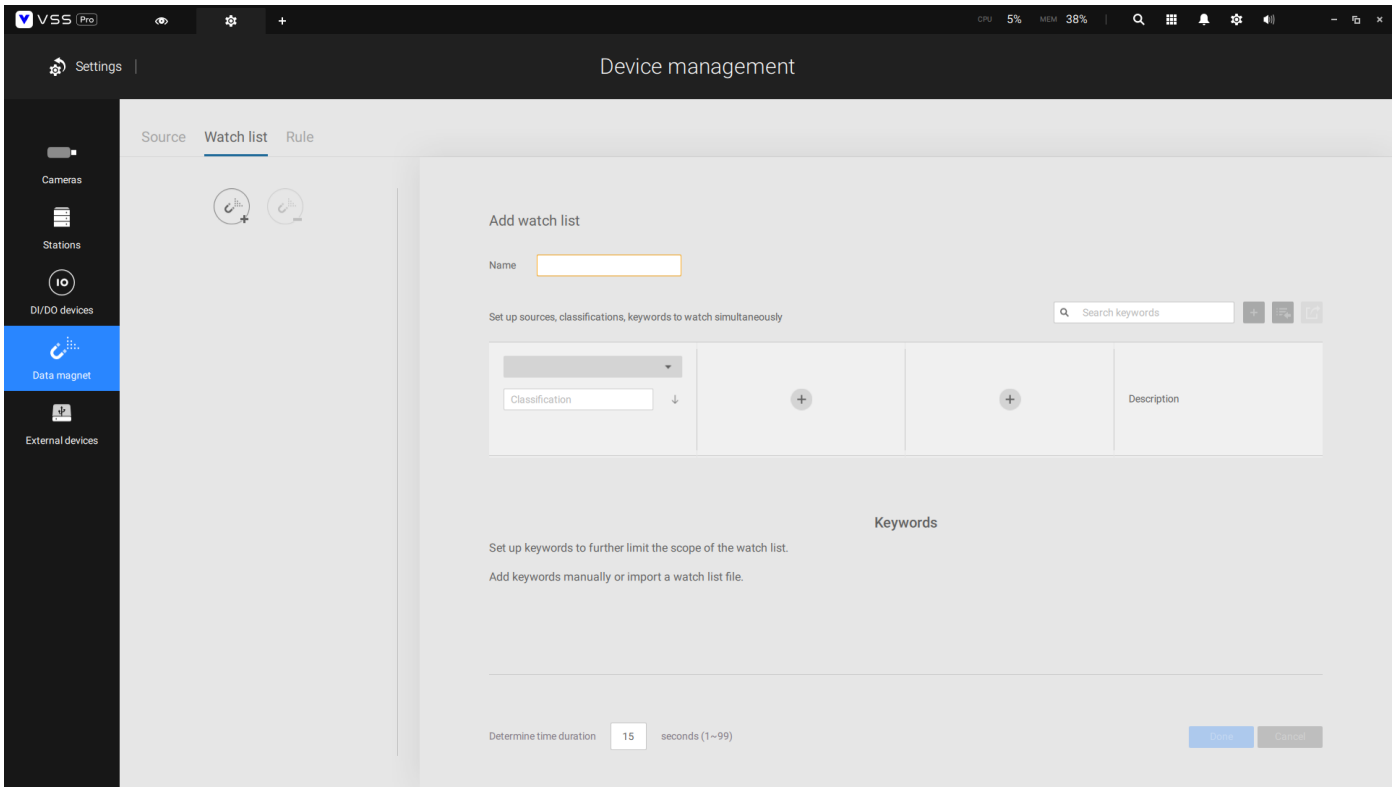
After setting up the Data source, you can go to the live view screen of the camera to which the Data source is connected. Then, click the right mouse button to call up the menu and select Data magnet. Check Show Data to call up the Data Magnet data display column. When the data source has transferred data to VSS, the data will appear in this field. The data and order displayed in the field can be set in Edit display data.

10. 

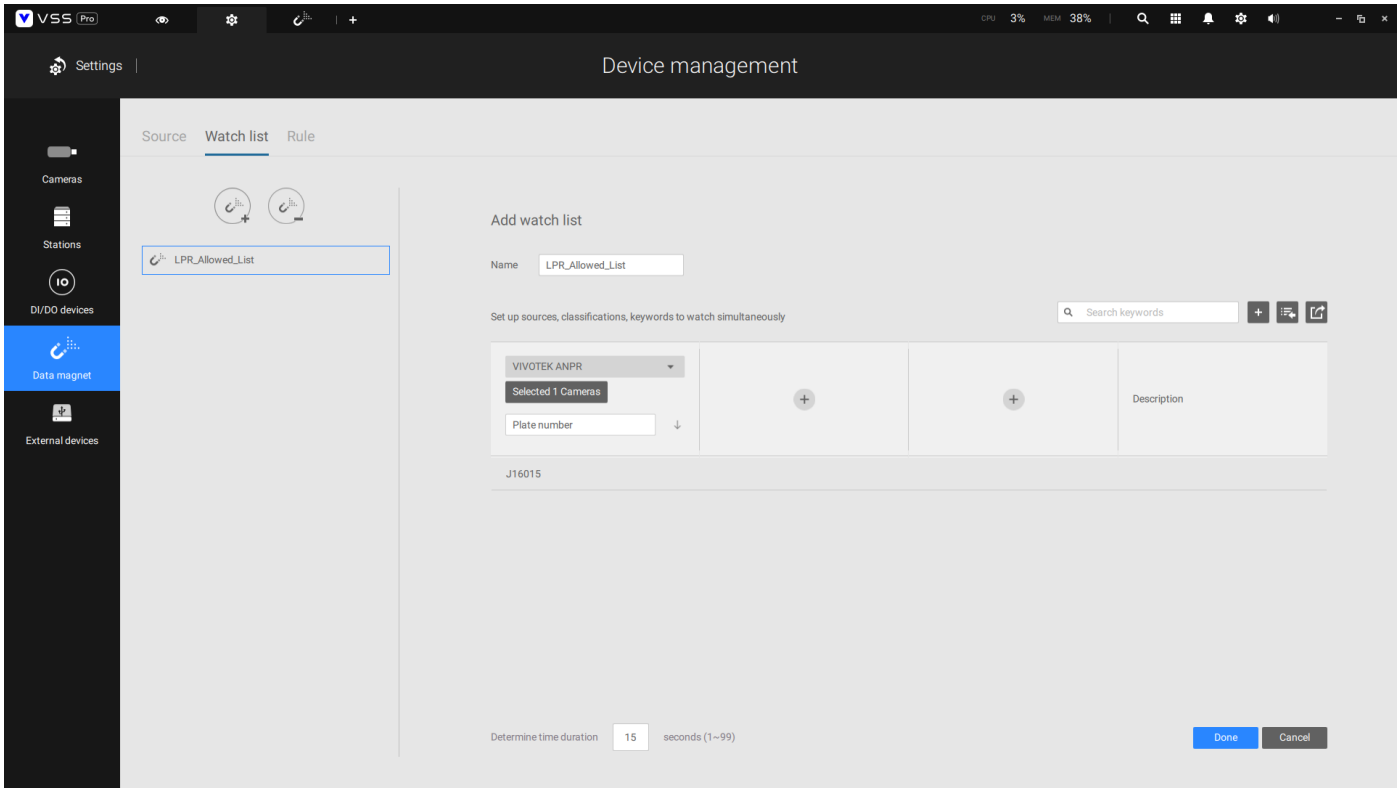
Watch List Trigger Actions

To use the Watch List trigger action, firstly go to Settings > Data Magnet > Watch list.
The function of the Watch list is to let the system monitor the data of different fields sent from the data source. First, select the source and classification you want to monitor, and then enter whether you want to monitor a certain keyword sent by that classification. If you do not enter a keyword, it will be triggered as long as the classification you input has sent in data.

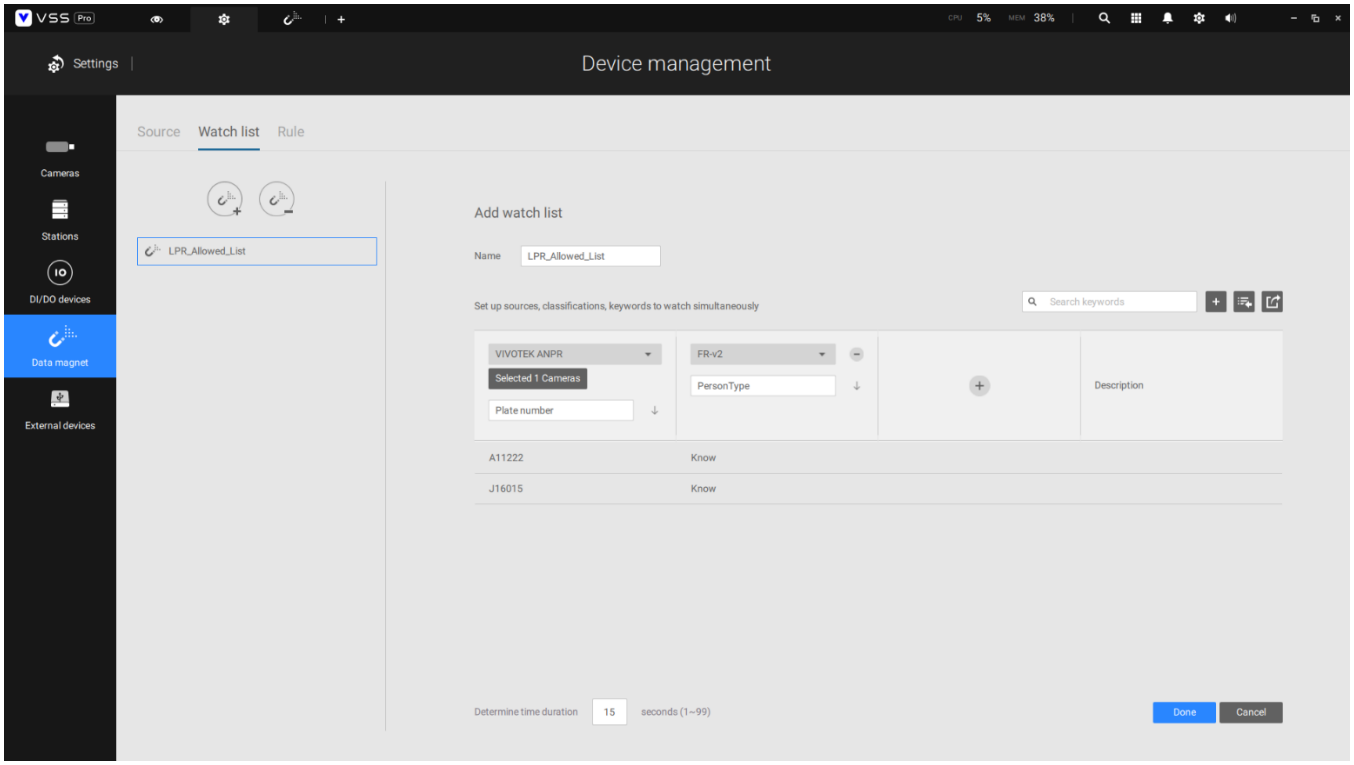
The fields of Classification must refer to the field definitions at the Data source end, and the classification defined by each data source is different.

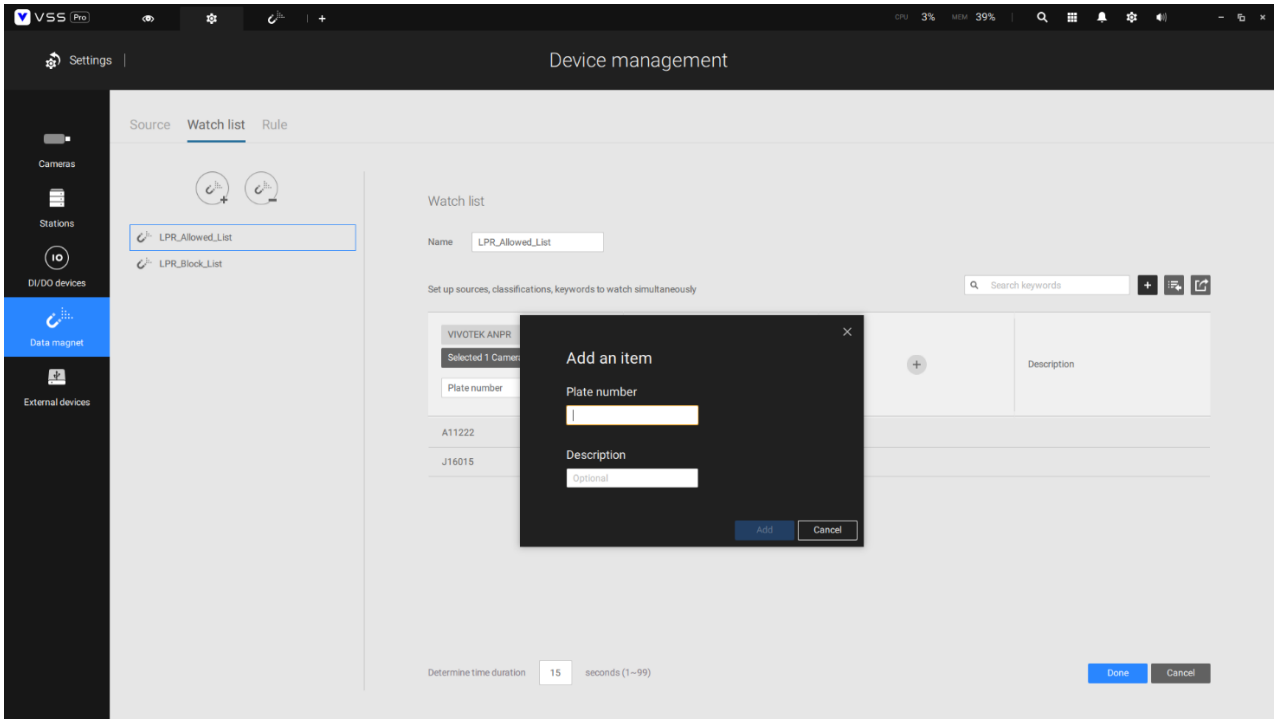


Take the VIVOTEK LPR camera as an example; assuming that you want to observe the plate number, enter the plate number in the classification field, and if you want to monitor vehicle number J16015, then enter J16015 in the keyword. Thus, when the VIVOTEK LPR Camera sends this vehicle number to VSS, the watch list will be triggered. If you want all vehicle numbers transmitted in VSS to be triggered, you don't need to input any data for the keyword.



Suppose you want the trigger to happen only when the data of two different data sources meet the conditions at the same time. In that case, you can enter the conditions for the second data source to monitor in the second field of the watch list.

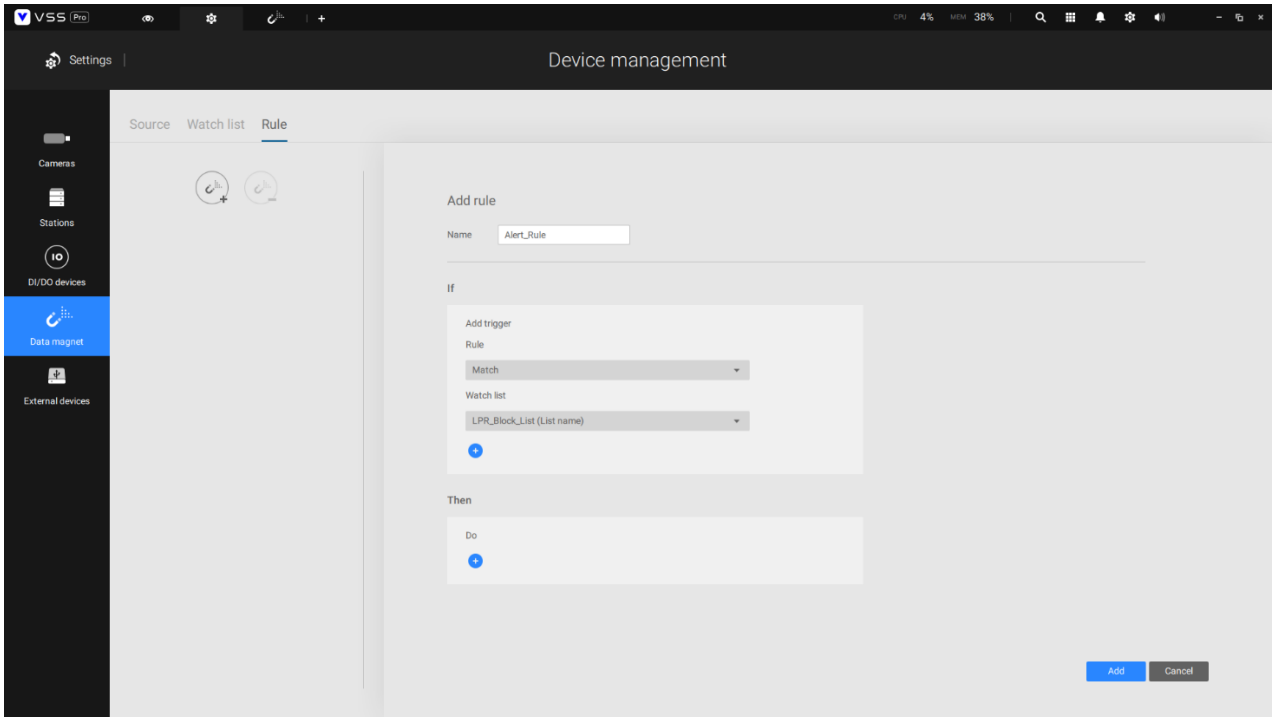


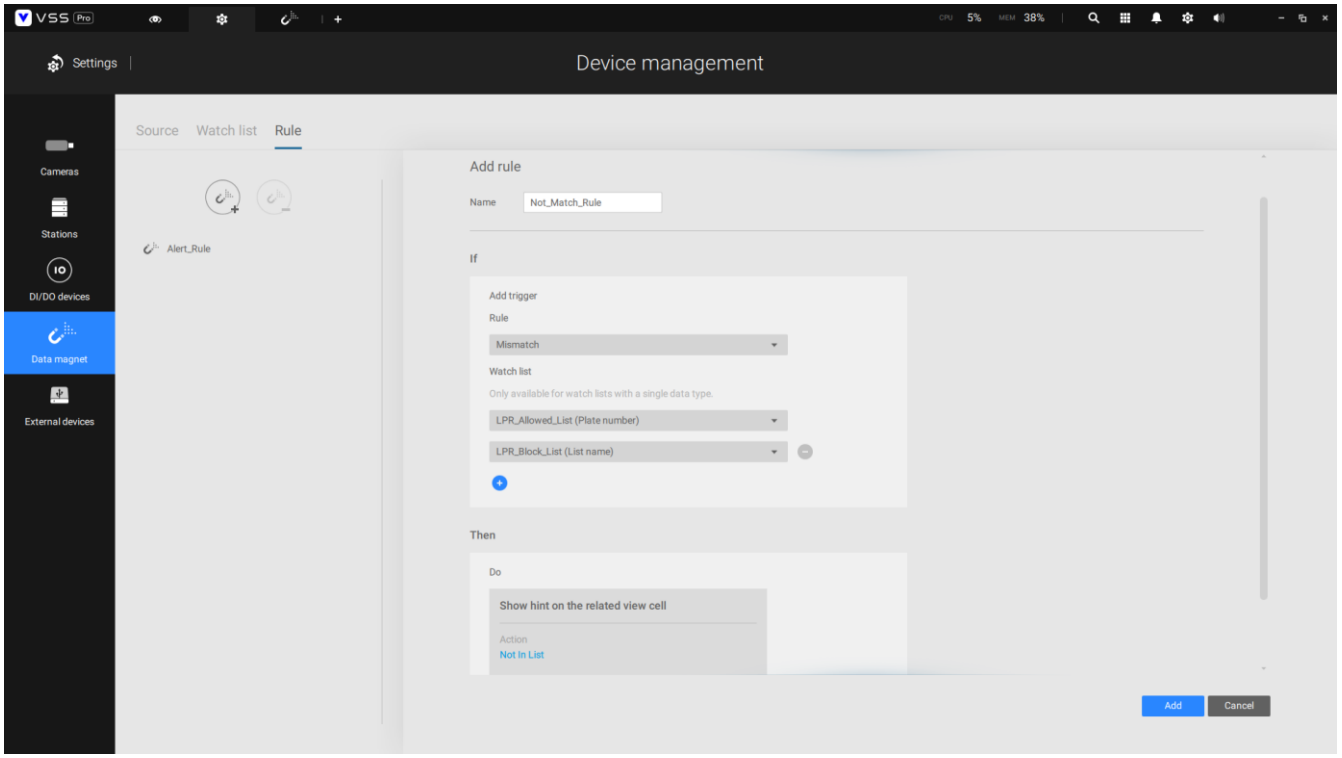


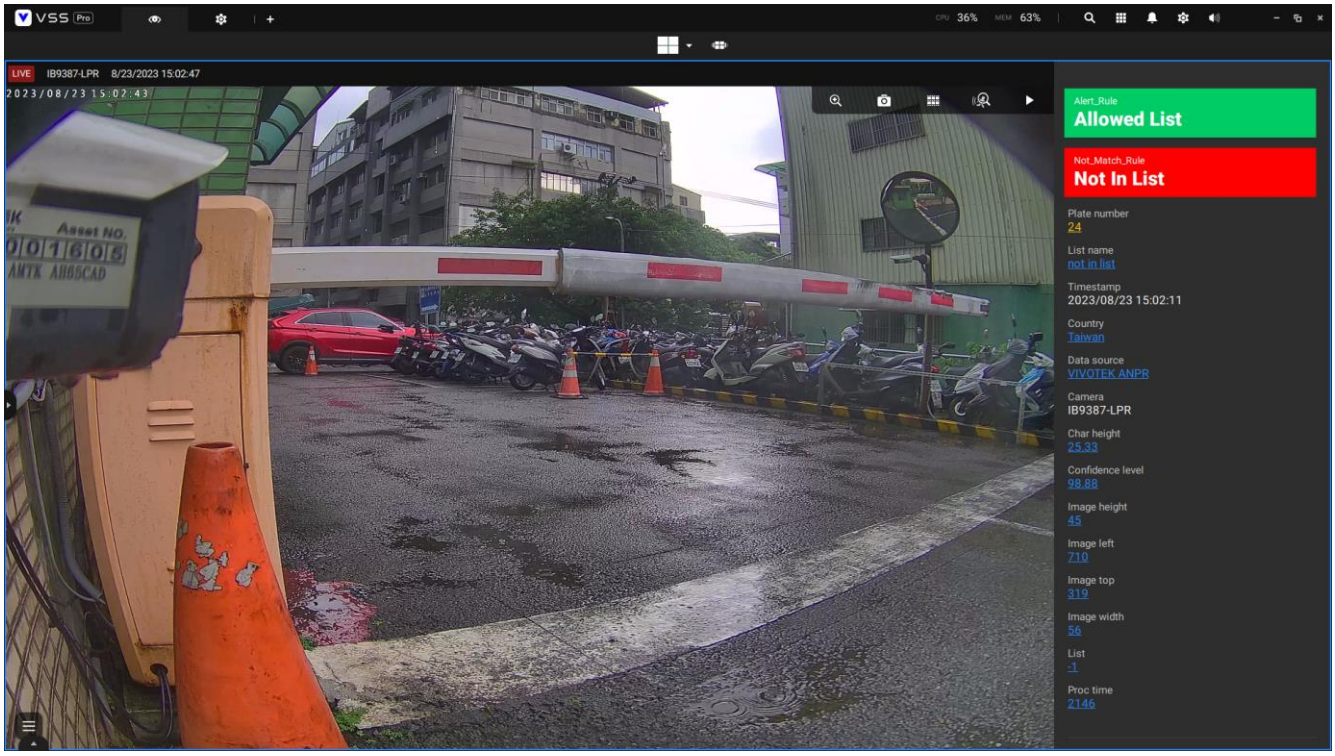
After the Watch List is triggered, there are two places where you can set what to do after the triggered action. The first one is the Rule.

Firstly, set Add trigger under If to decide how to trigger when there is a match or no match in the data of the watch list. Then, select which watch list to match. If you select two watch lists to match, any watch list having a match will trigger. If you select two watch lists to unmatch, the trigger will happen when the data in the two watchlists does not match.

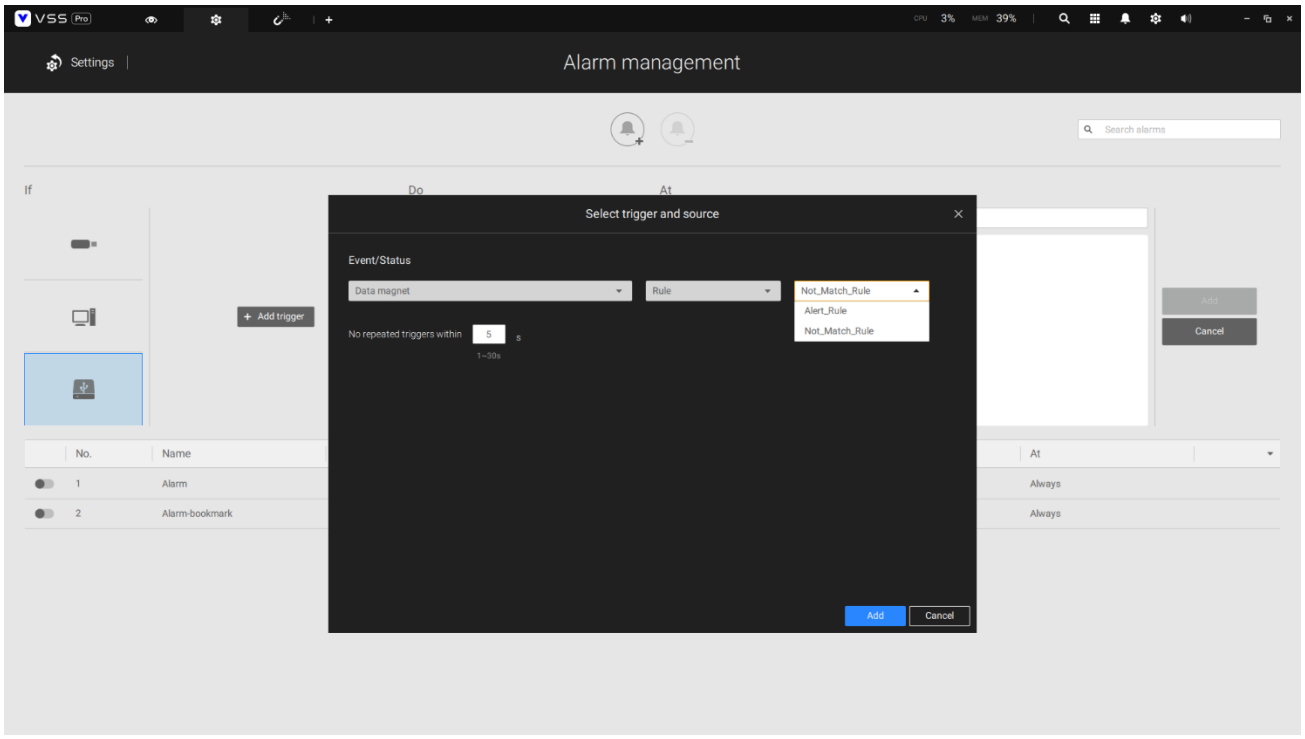
Secondly, set what action to execute after the Do setting under Then is triggered. Currently, two actions are supported. The first one "Show hint on the related view cell" is to display a more obvious hint on the camera live view (like the red and green boxes on the right of the window). The second "Select data to send to Wiegand converter" is to send the triggered data (such as the car number mentioned earlier) to the Wiegand converter added to VSS external devices.




VSS Pro
CPU 5% MEM 38%
Settings
Device management
Cameras
Stations
DI/DO devices
Data magnet
External devices
Source
Watch list
Rule
Alert_Rule
Add rule
Name
Not_Match_Rule
If
Add trigger
Rule
Mismatch
Watch list
Only available for watch lists with a single data type.
LPR_Allowed_List (Plate number)
LPR_Block_List (List name)
Then
Do
Show hint on the related view cell
Action
Not In List
Add
Cancel

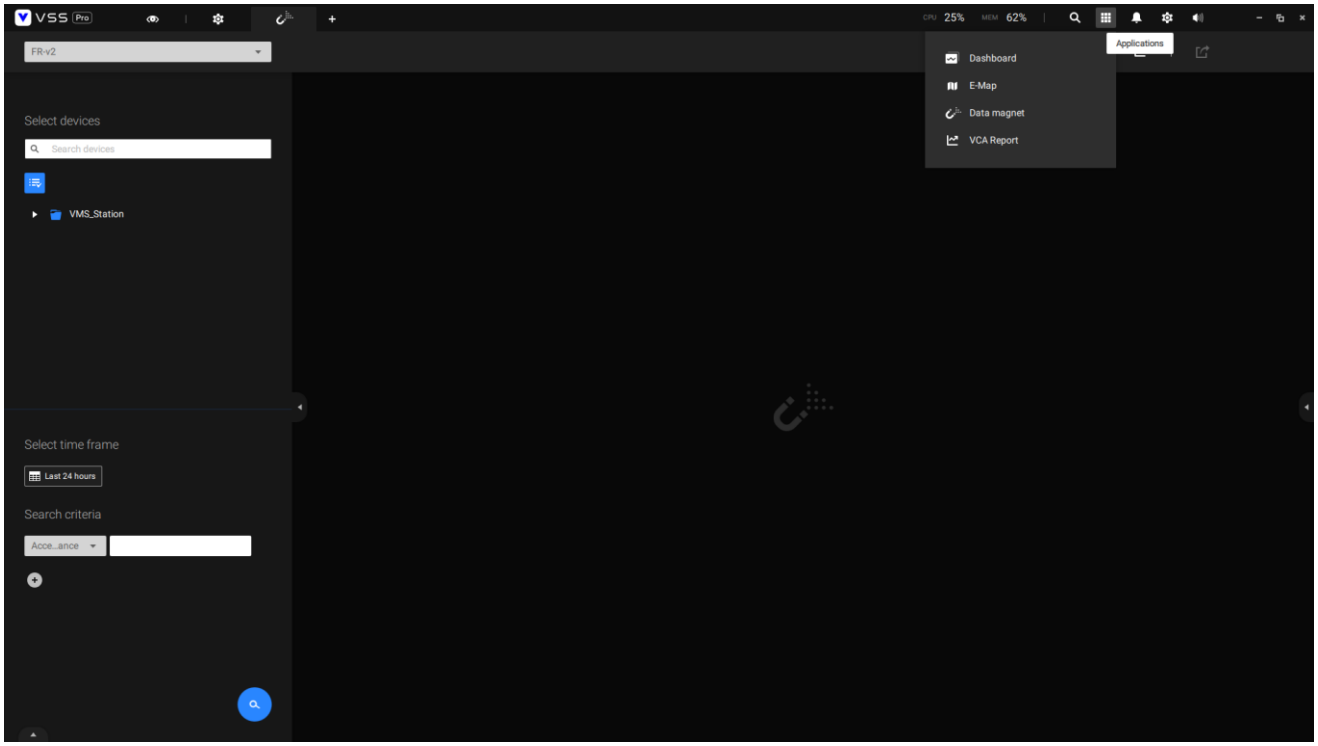

VSS Pro
CPU 36% MEM 63%
LIVE
IB9387-LPR
8/23/2023 15:02:47
2023/08/23 15:02:43
Alert_Rule
Allowed List
Not_Match_Rule
Not In List
Plate number
24
List name
not in list
Timestamp
2023/08/23 15:02:11
Country
Taiwan
Data source
VIVOTEK ANPR
Camera
IB9387-LPR
Char height
25.33
Confidence level
98.88
Image height
45
Image left
710
Image top
319
Image width
56
List
-1
Proc time
2146

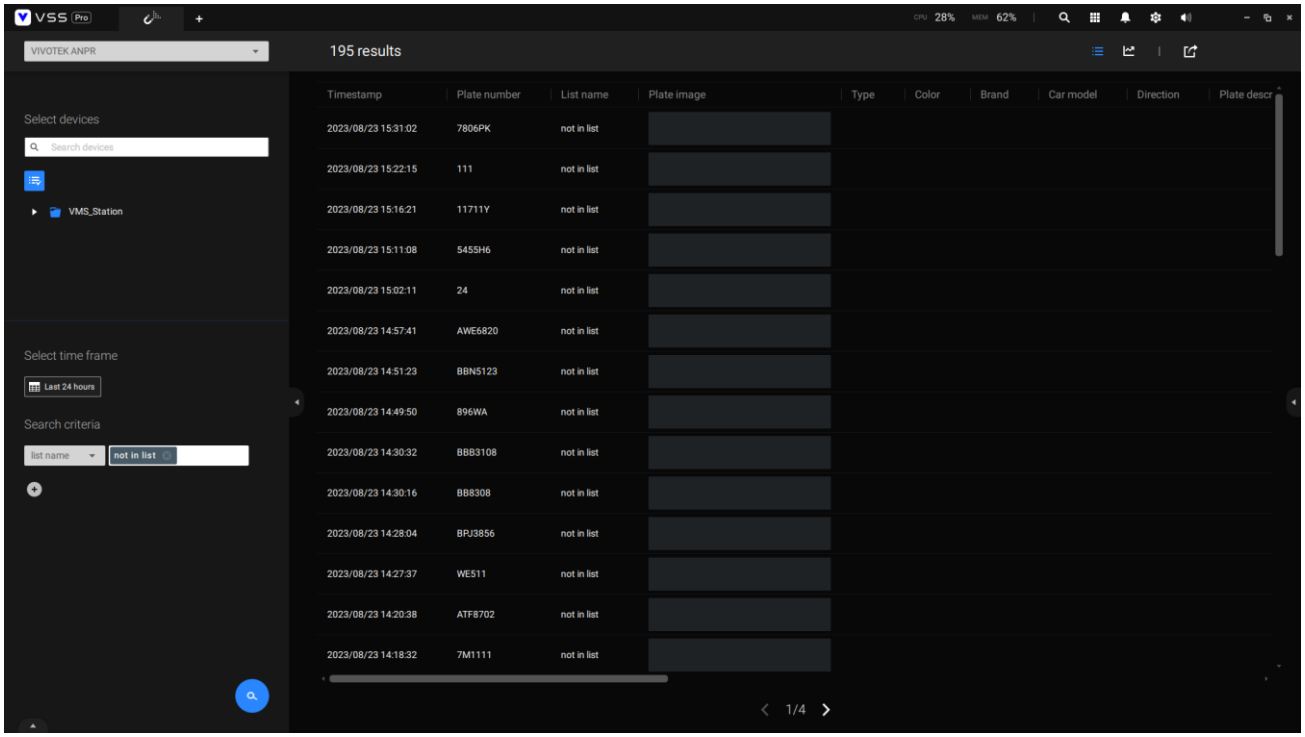
Another action that can be triggered is in Alarm management.
Go to Settings > Alarm > Add an alarm, then select External device event under If and select Data magnet under Add trigger. Now, you can choose whether to use the rule or the data of a certain field as the alarm trigger. Then, you can select the actions alarm management supports.



Dat Magnet Search

Run Data magnet from the Applications in the title bar on the upper right, and the Data Magnet Search function will appear. You can select the data source, devices, time, or search criteria to search for the data transmitted by the data source.





3-5. Managed PoE Switch

Introduction

Starting from VSS version 1.2, users can integrate VIVOTEK Managed PoE switches as External devices into VSS. This integration allows users to access several functionalities of the PoE switch through VSS, such as controlling the PoE on/off of each port, viewing the topology of the switch connected to cameras, and monitoring the overall network traffic of the switch. This feature assists users in monitoring traffic for cameras through the PoE switch and in conducting basic troubleshooting.

Configuration

Before starting to use the integration features of the Managed PoE Switch, users must first add the PoE Switch to the VSS External device. Users can navigate to Settings > Device > External device > managed PoE switch, click the Add PoE Switch button as shown in Figure 1, and add a new PoE switch. In Figure 2, users can input relevant information about the PoE switch, including the device name, IP address, connection port, login username, and login password. It is important to note that the PoE switch must be in the same network segment as the VSS server to be discovered. Additionally, this integration only supports VIVOTEK brand-managed PoE switches, so please refer to the support list in the datasheet for compatibility details. You can also delete the existing PoE switch by clicking the delete PoE switch button.

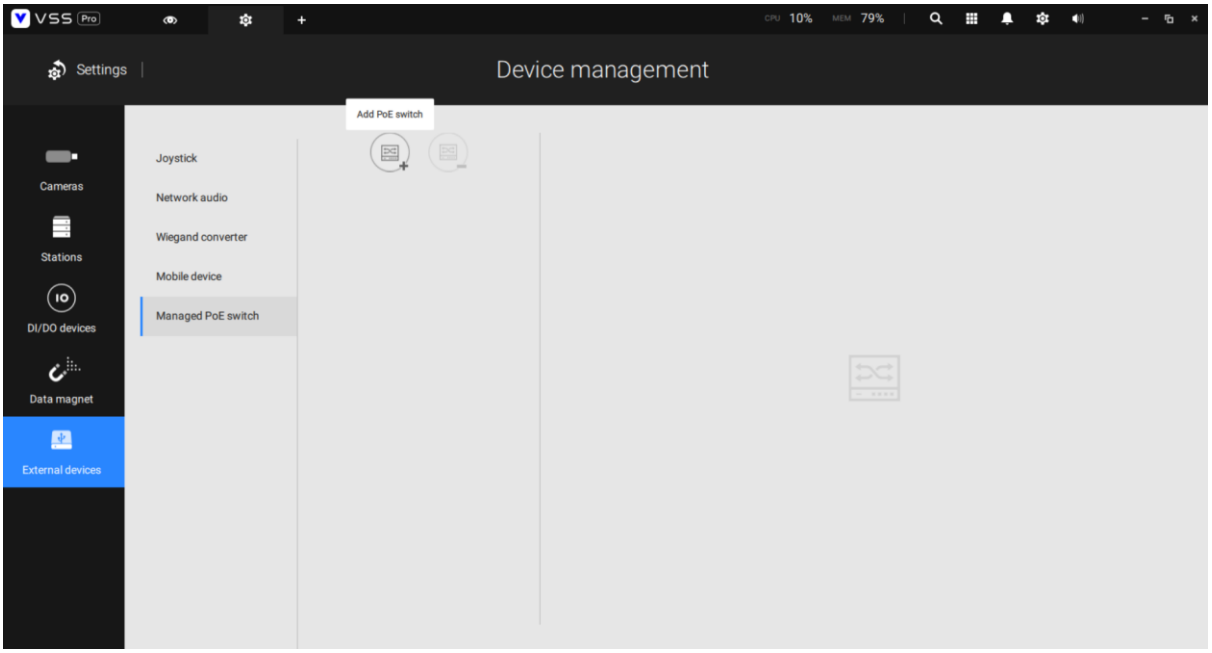


Figure 1

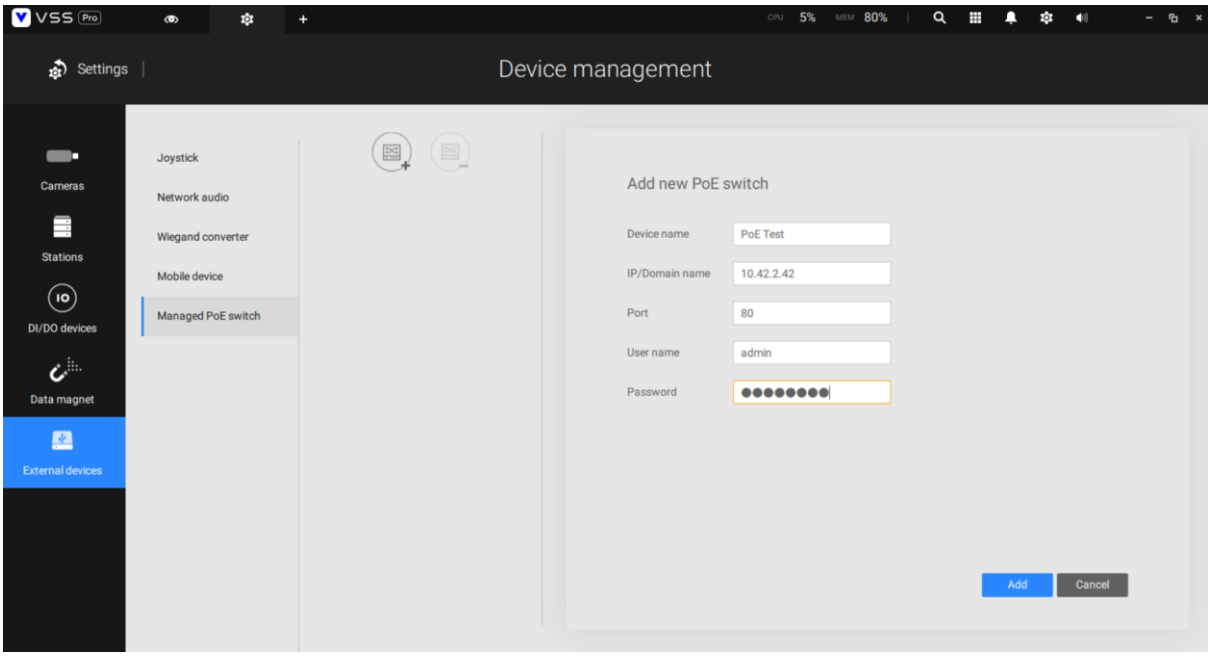


Figure 2

Operation

After adding the PoE switch to VSS, you can click on the PoE switch, and on the right-hand side, you will see the information and related integration web pages for that PoE switch, including PoE on/off, Topology view, and traffic monitor. It is important to note that some VIVOTEK Managed PoE Switches only support the PoE on/off page as shown in Figure 4.

Under the information page, you can see basic information about the PoE switch, including Device name/model name, IP address, MAC address, connection port, and firmware version, as shown in Figure 3.

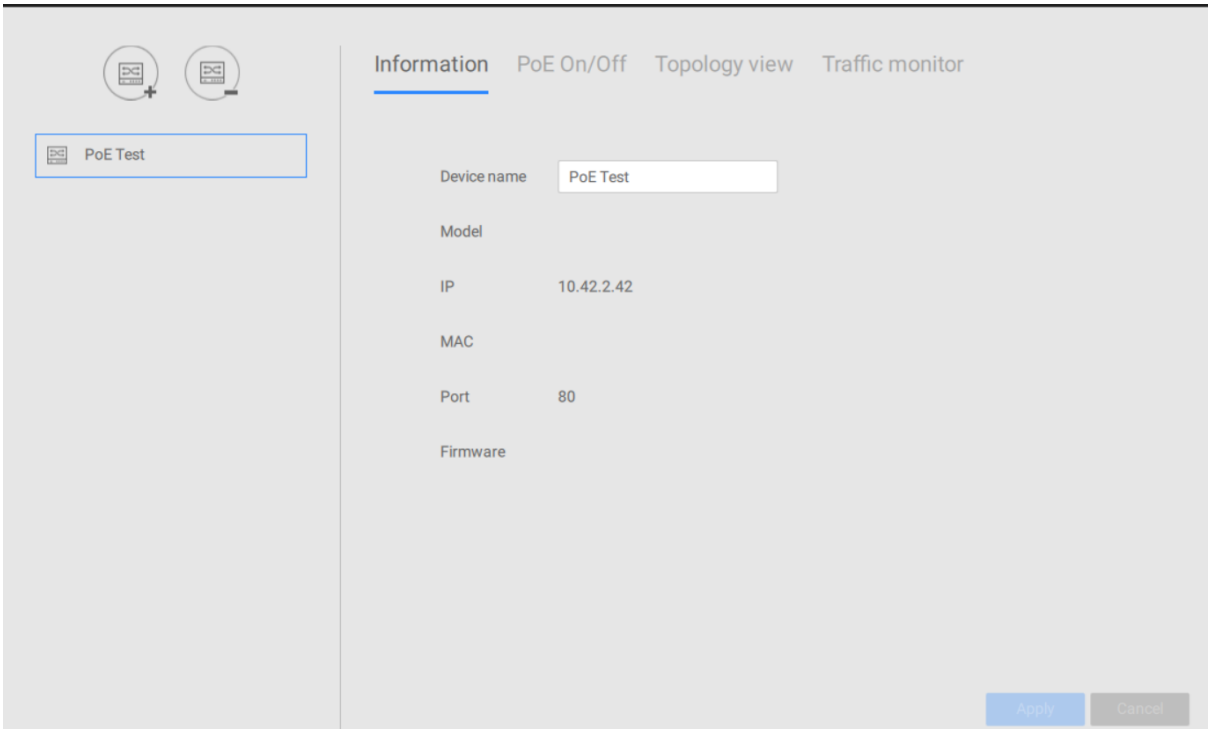


Figure 3

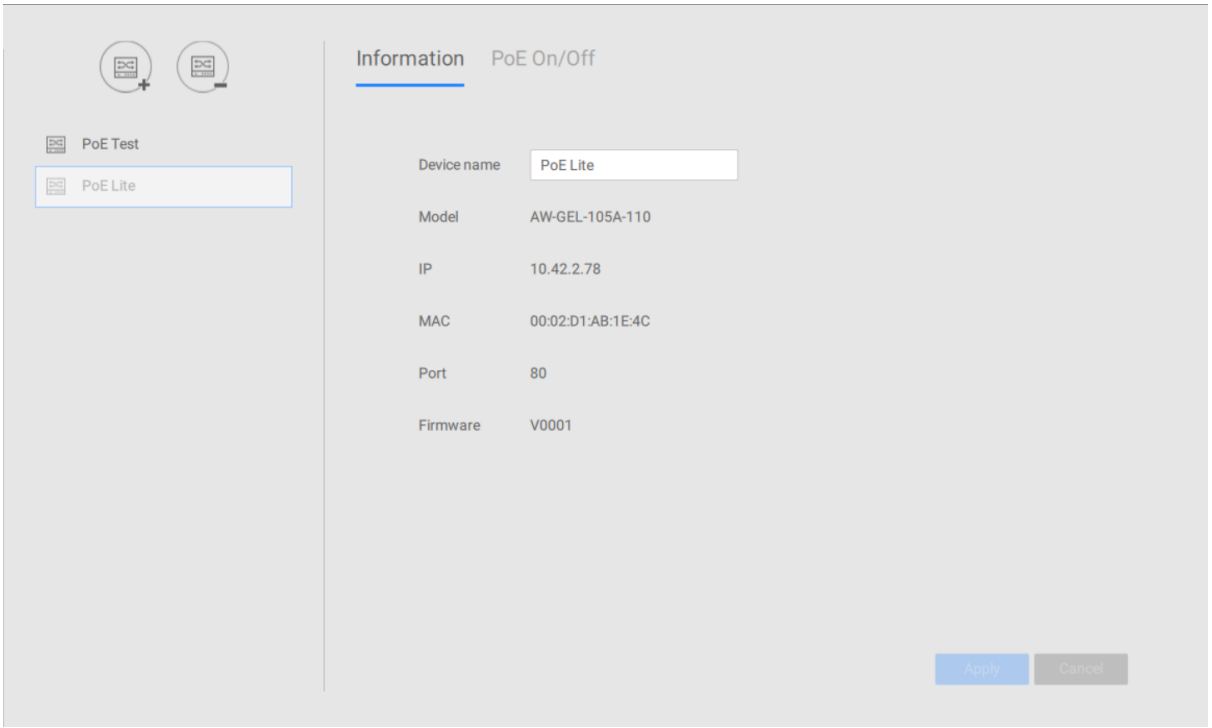


Figure 4

Clicking on the PoE On/Off page, as shown in Figures 5 & 6, you can access the PoE On/Off webpage for that particular switch. On this page, you can control the on/off status of all PoE ports and view the PoE usage status of each port.

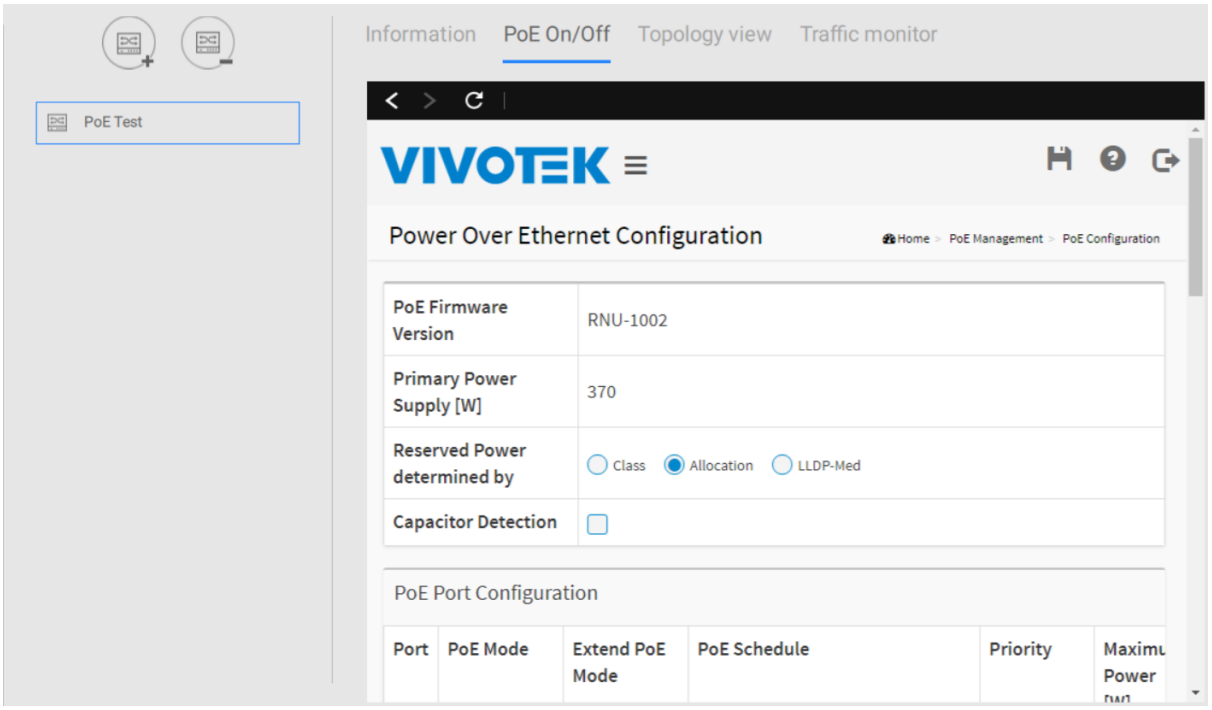


Figure 5

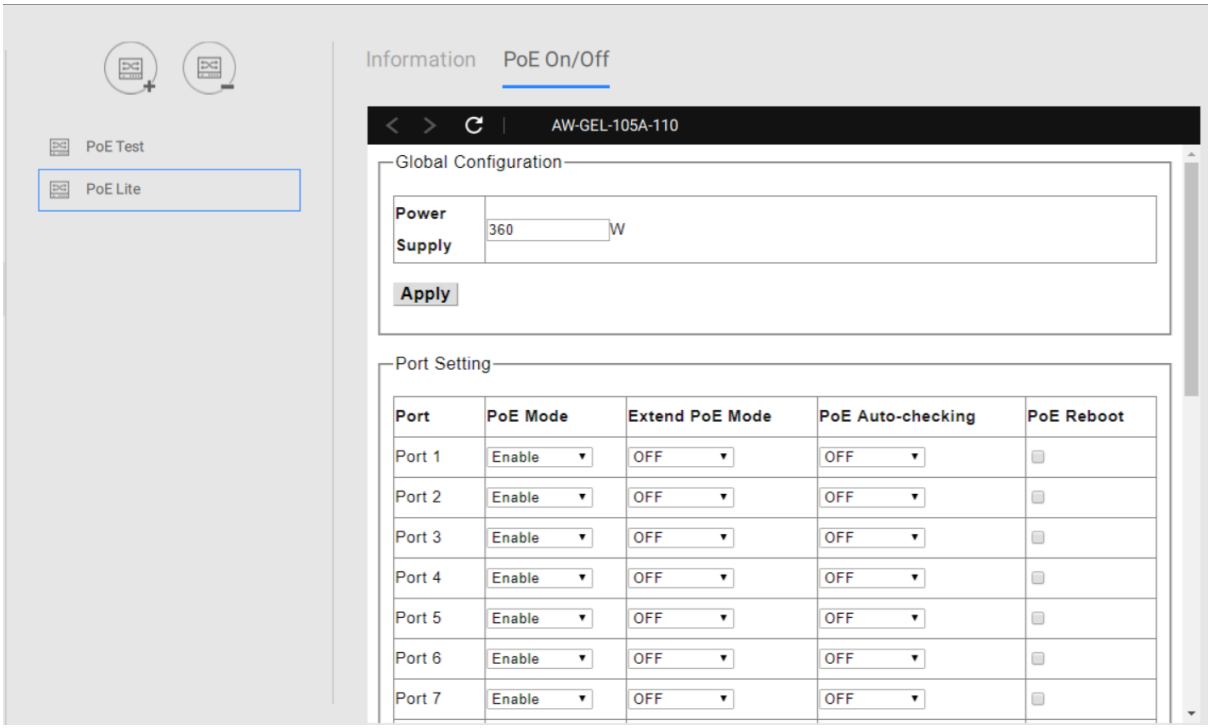


Figure 6

On the Topology view page, as shown in Figure 7, you can view all the connected cameras or devices of the switch, and you can operate basic troubleshooting for the connected cameras, including reboot/diagnostic.

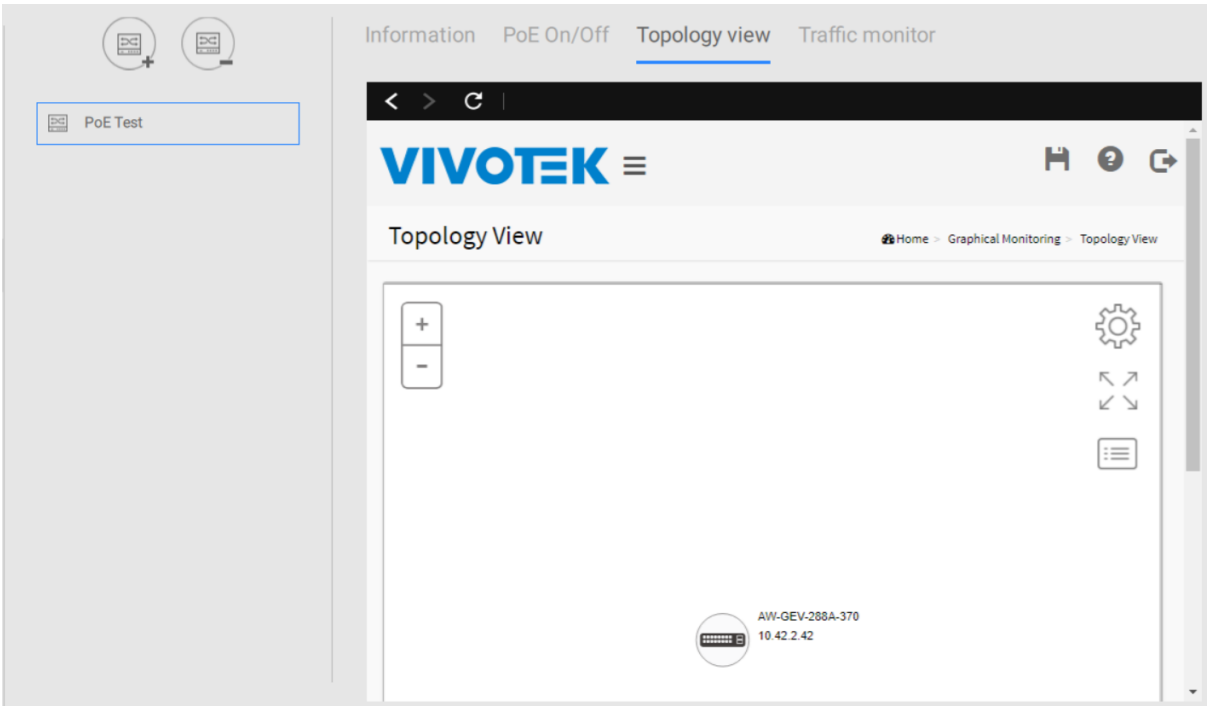


Figure 7

On the Traffic monitor page as shown in Figure 8, you can monitor network bandwidth for each switch port.

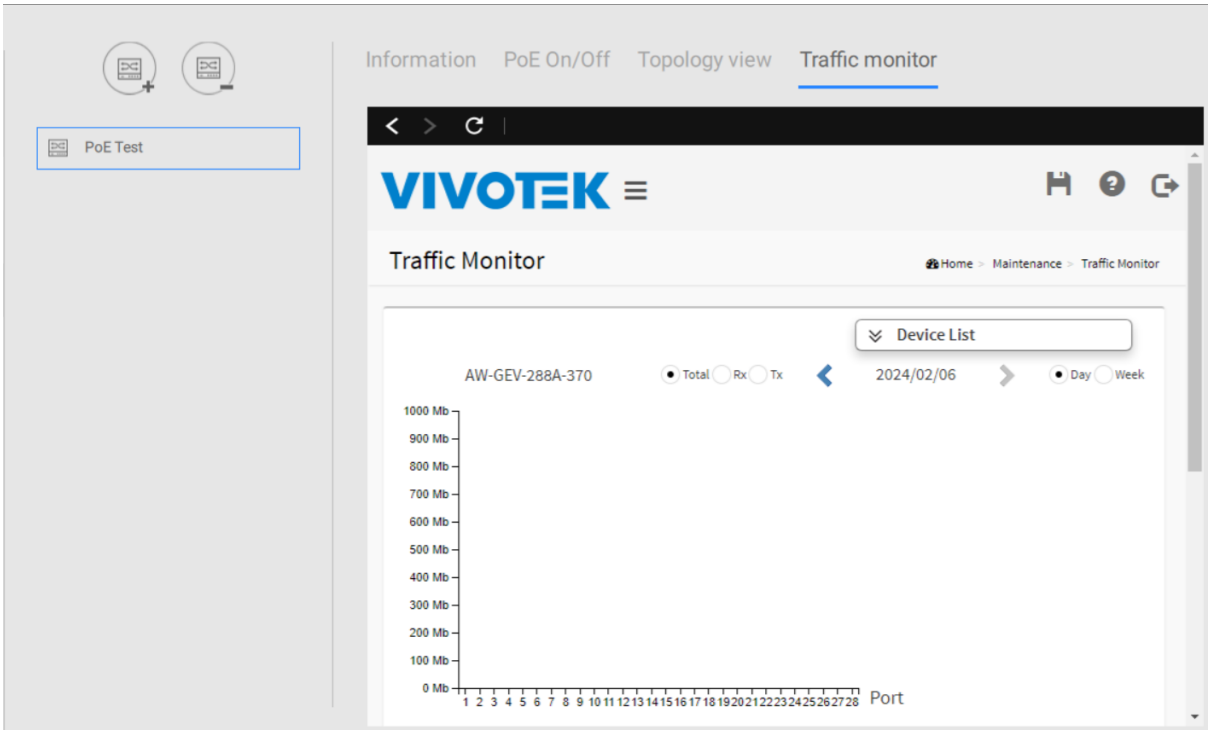


Figure 8

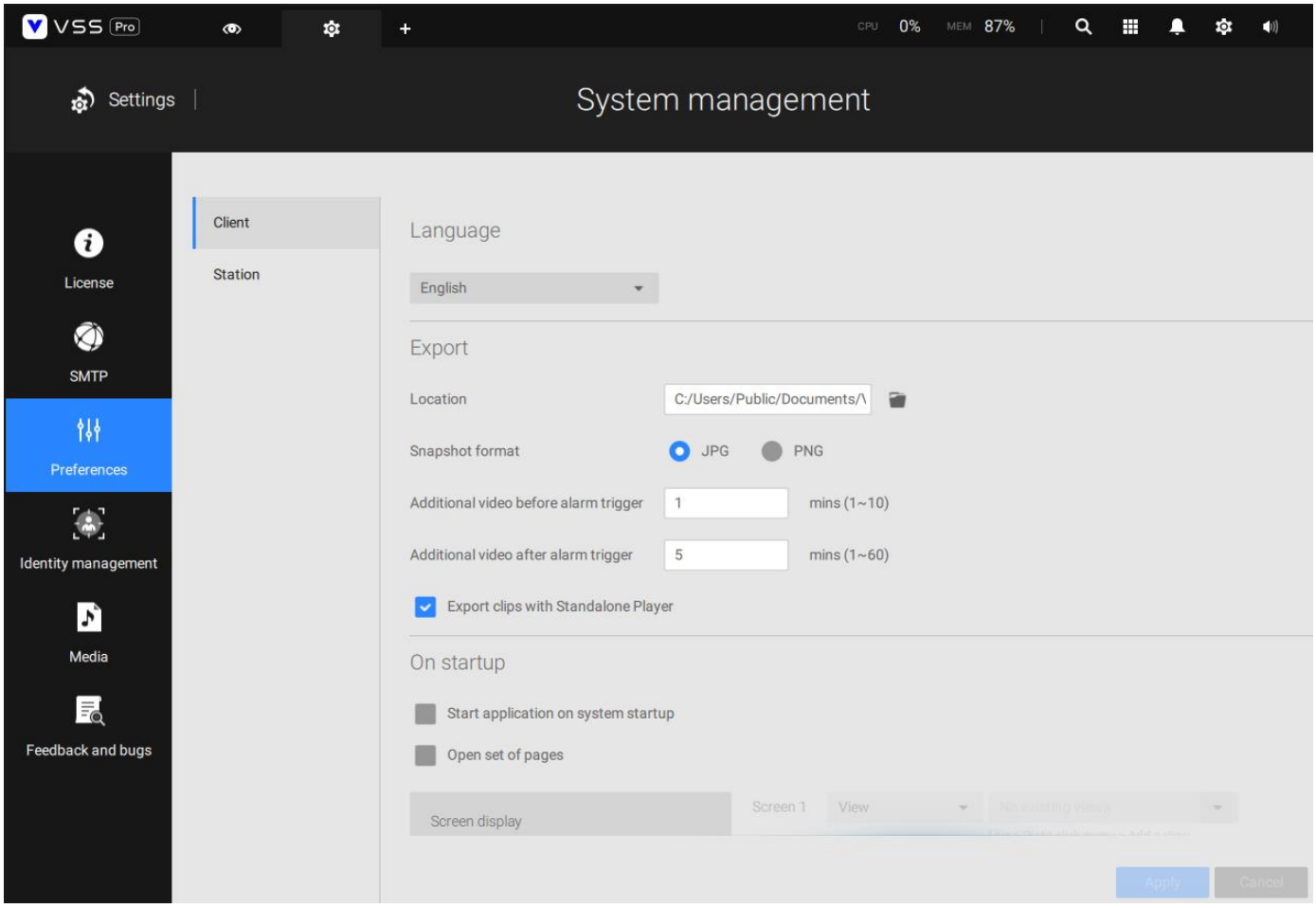
Chapter 4: Settings

4-1. Settings > System > Preferences

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

Client Setting:

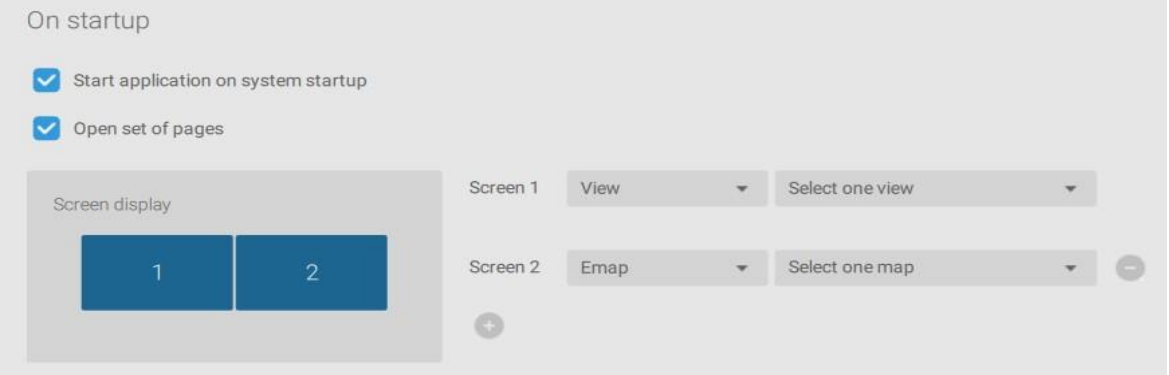
1. Select the UI text language.
2. Configure a default destination for exporting video, snapshots, or configuration backups. The default is "C:\Users\Public\Documents\VIVOTEK Inc\VAST\Downloads". You can change the media format via the checkboxes.
3. Select the format for the snapshot as either JPG or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



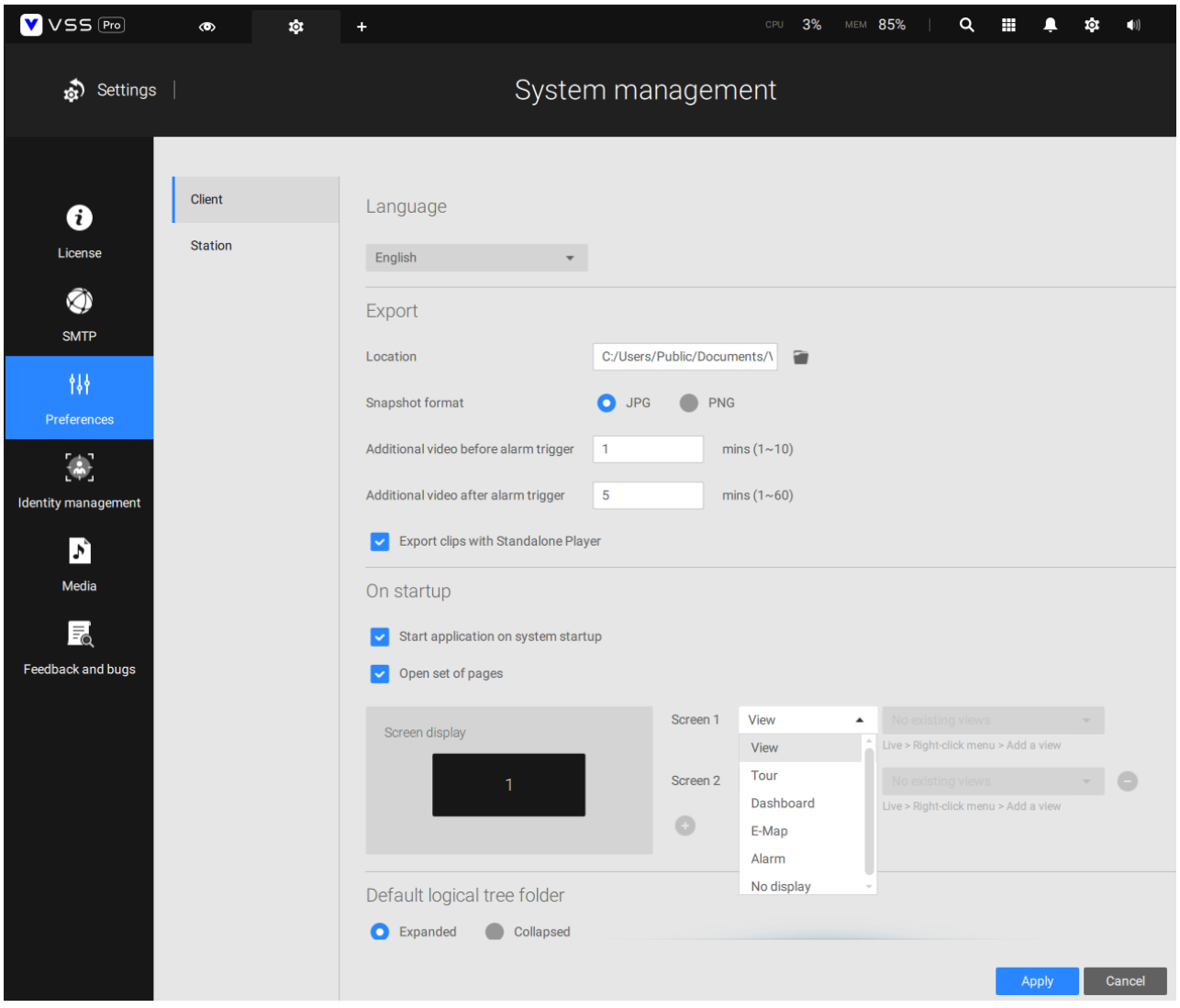
6. The default Live view, which may span across multiple monitor screens and display Live view, Tour, Dashboard, E-Map, or Alarm prompts. The precondition is that you should configure one or many views before making the Startup configuration.

   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.



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



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.

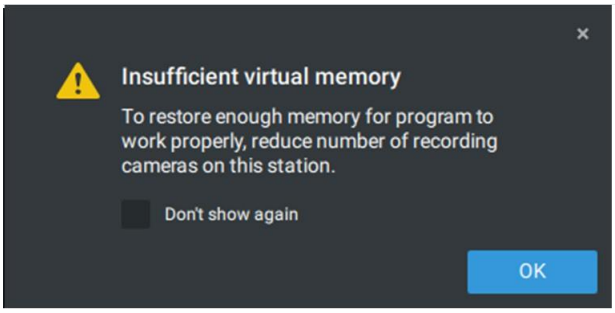
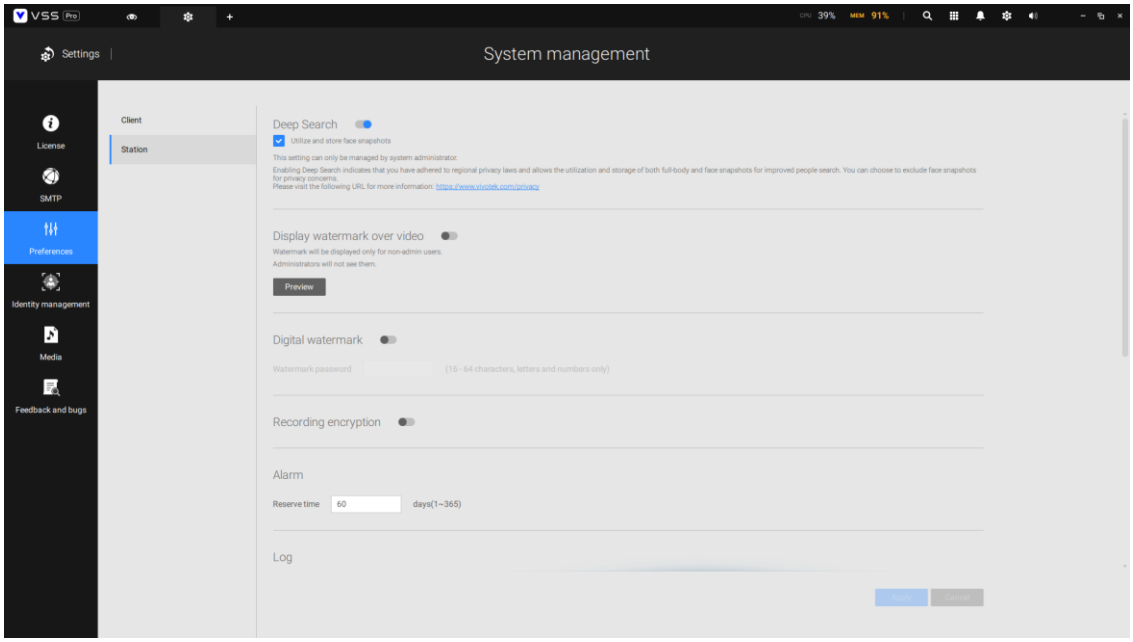


Image resampling method: Select a resampling method if the need should arise.

Click the Apply button for the configuration to take effect.

Station Setting:

1. **Deep Search** - Only users with an admin account can see and manage this setting. Turning it on allows VSS to utilize and store person attributes and full-body/face images for improved people search. Additionally, you have the flexibility to decide whether to enable or disable VSS from utilizing and storing face snapshots based on your specific needs. The stored data will be recycled with recordings based on the recording recycle setting. Before turning it on, ensure compliance with regional privacy laws and obtain consent from individuals for using their attributes and images if required. Once the Deep Search function is turned off, Deep Search cannot function, and the Deep Search icon on the view cell for the VIVOTEK AI cameras will be switched to the Smart Search icon. Note that the setting will not be applied successfully if the software versions among clients and servers are incompatible.



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

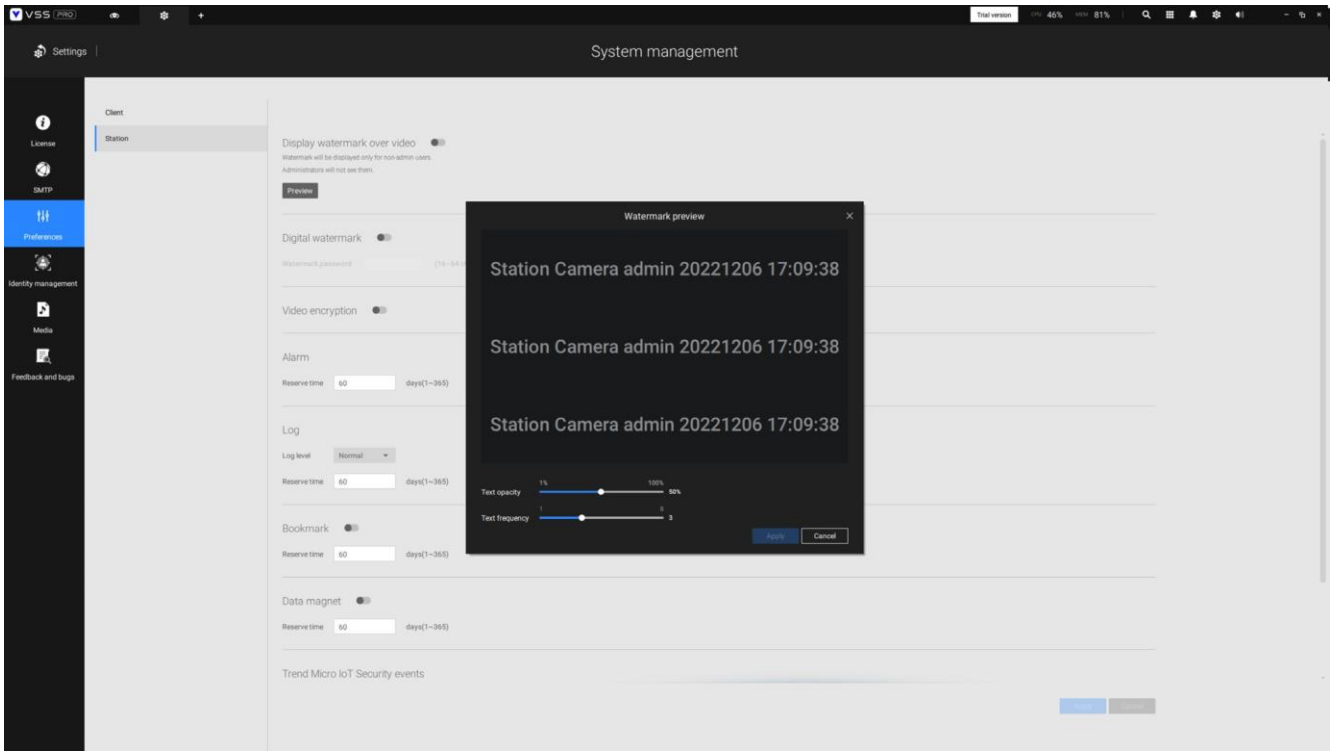
   Encrypted watermark for authentication:
   To ensure your video is authentic and has not forgerized, adding an encrypted watermark on the data stream can be achieved with a customized password. You can use the Standalone Player to verify which frames in the video footage have been tampered with.

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

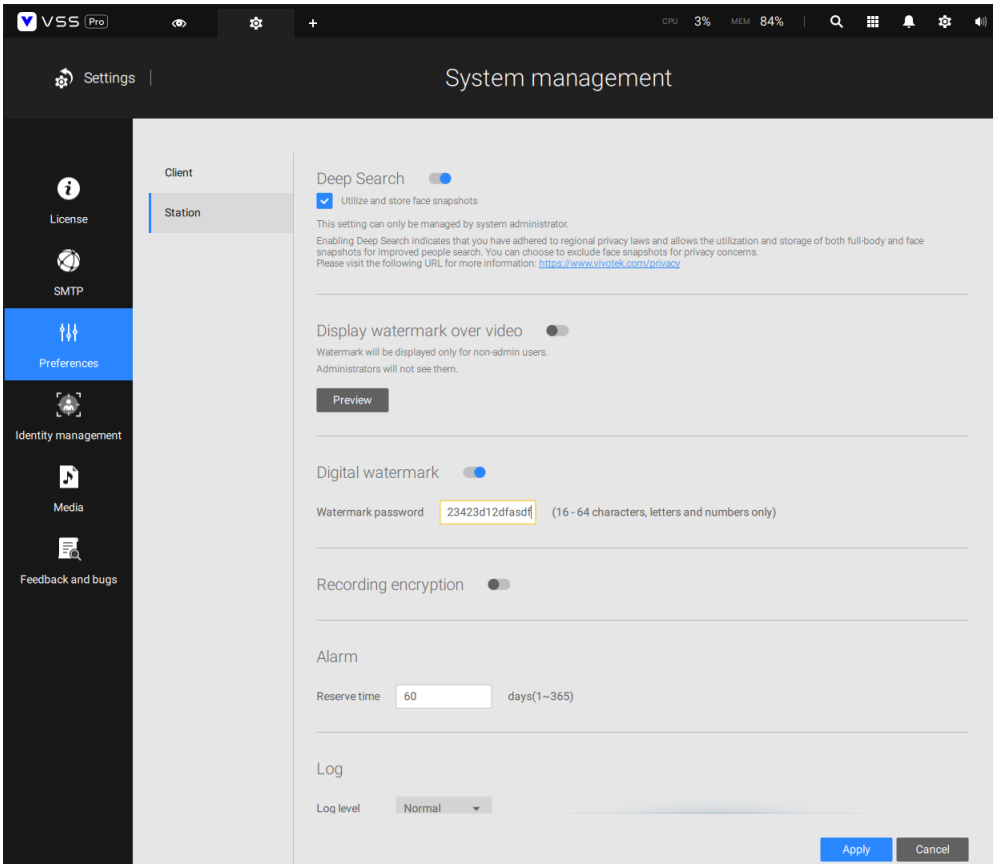
3. **Digital watermark** - To prevent forgery of recorded or exported video clips, and to prove the validity of surveillance evidence, digital watermark can be appended to recorded video.

   Note that only non-administrator users will see watermarks.

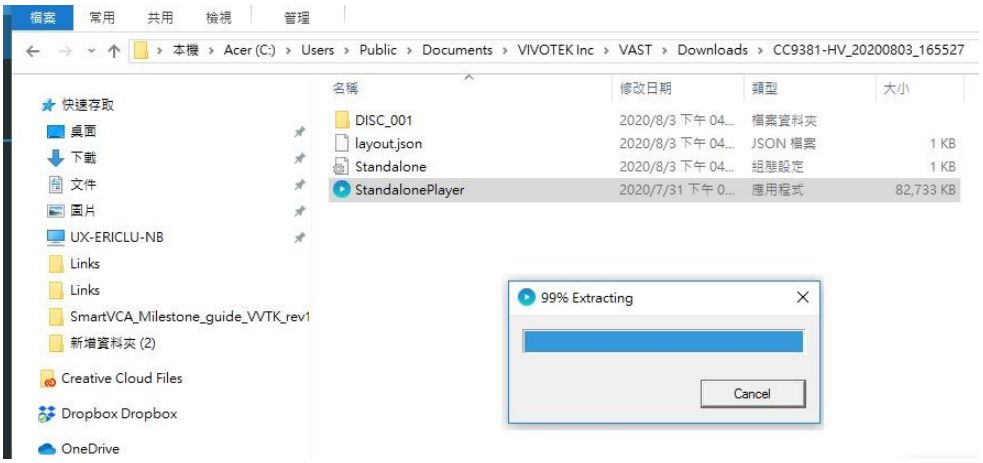
   To enable the text watermark, use the slide button. Use the Preview function to tune the text opacity and text frequency display on the screen.



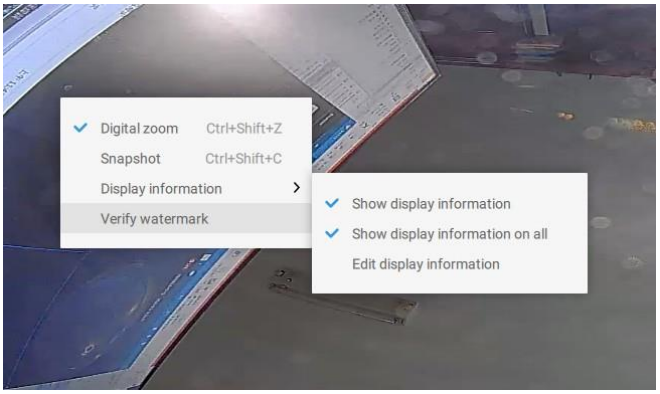
To enable Digital watermark, enter a password that is at least 16 characters long. Once a valid password is available, you can click the Apply button to preserve your setting.



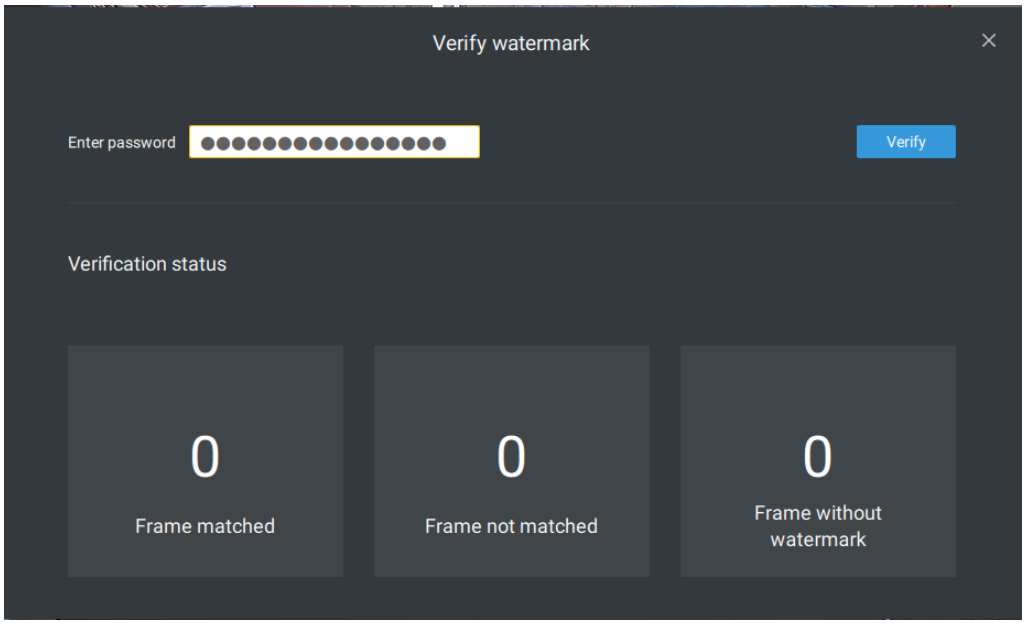
When you export a video clip, a StandalonePlayer is generated with the exported files.



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



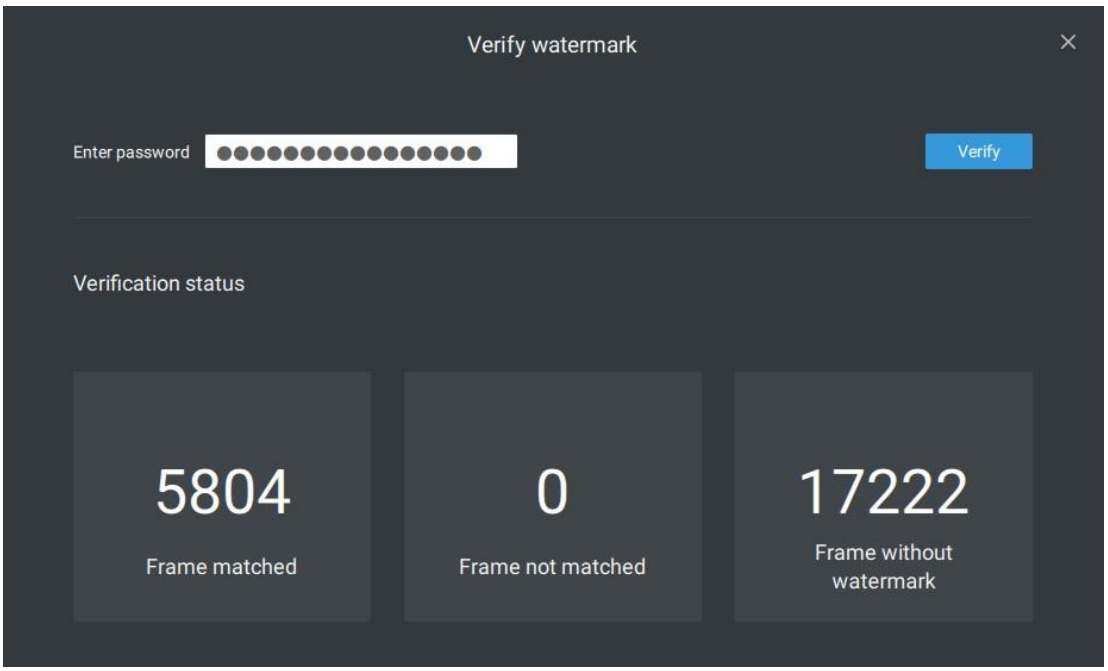
The Verify screen will display. Enter the pre-configured password. Click Verify.



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.



4. **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.
5. **Log**: Use the menu to configure the preservation time of the Major, Normal, or Minor logs.
6. **Bookmark**: Configure the days of preservation for bookmarks.
7. **Data magnet**: Configure the days of preservation for data related to Data Magnet.
8. **Trend Micro events**: Configure the days of preservation for events related to cyber security.
9. **Database**: Configure the destination of the database folder. The database contains information for system log, alarms, Bookmarks, data magnet, Counting Reports, POS transaction data, snapshots, and Trend Micro IoT security information.

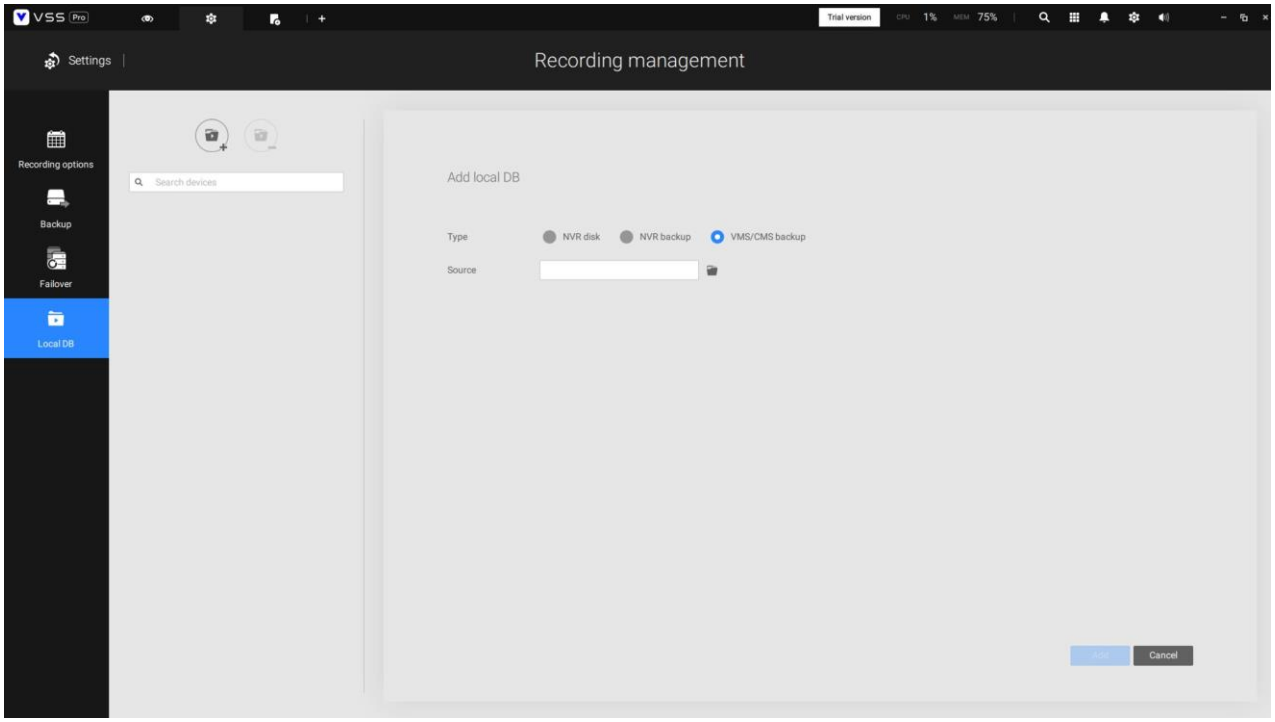
Recording Encryption - Recording encryption allows users to encrypt the recording videos with password protection. Playing the encrypted video on the original VSS server does not require entering the password.

Playing on other VSS servers or disabling recording encryption will require entering the password. The password is not able to recover or reset if you forget the original password.

Encrypted video files (.3gp) cannot be played in other media players. Please use the following two methods to view the video files outside the original VSS server.

1. Import to other VSS servers as Local DB

a. Copy the entire recording folder from the original VSS server to another location.
b. Enter Settings > Recording > Local DB in another VSS server.
c. Add local DB with VMS/CMB backup type.
d. The recording will be mounted as a local DB and listed sub-tree.



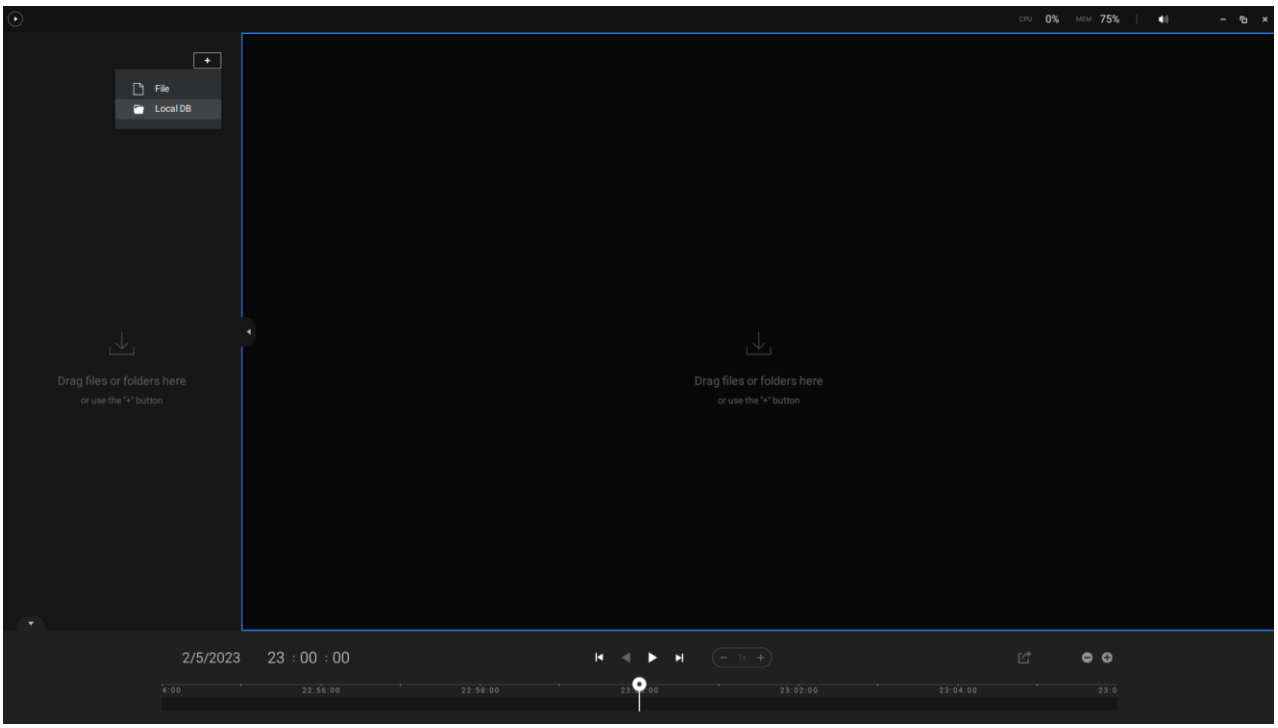
2. Import to VSS Standalone player as Local DB

a. Copy the entire recording folder from the original VSS server to another location.

b. Launch Standaloneplayer.exe in C:\Program Files (x86)\VIVOTEK Inc\VAST\Client\VSS\

c. Add local DB with VMS/CMB backup type by dragging the entire recording folder or using the “+” button.

d. The recording will be mounted as a local DB.



4-2. Settings > System > SMTP

Configure a mail server via which the system alarms or notifications can be delivered to a receiver.

Enter the Settings page, select 

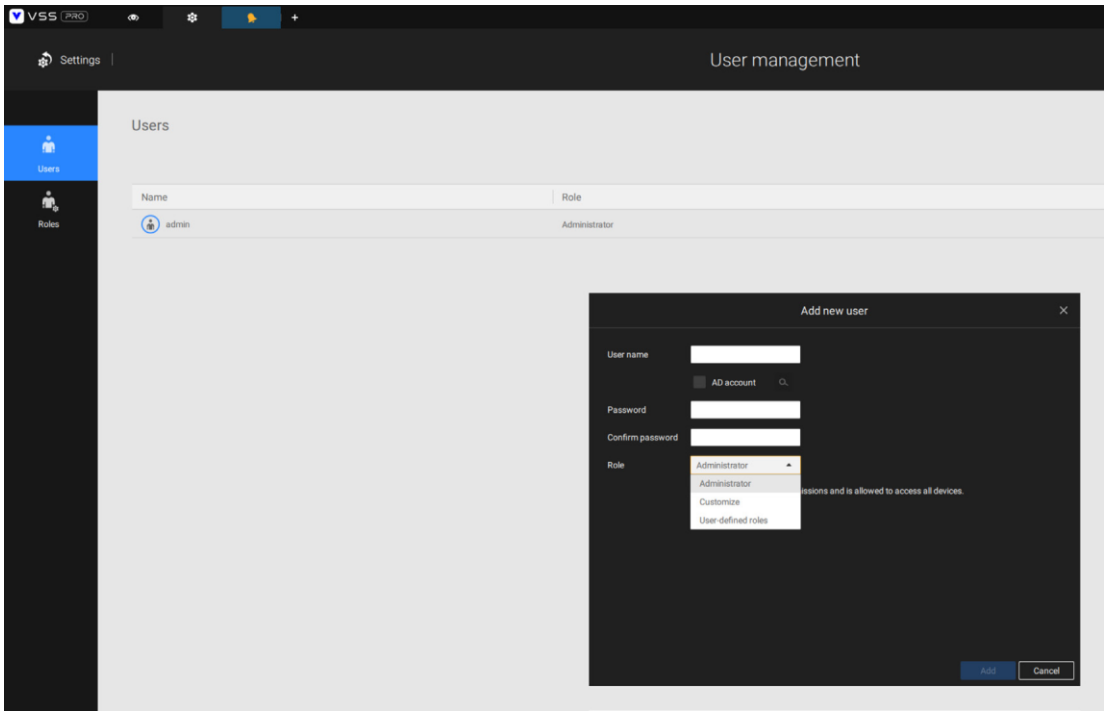
. Click on the Add SMTP button.
Enter your mail server's domain name or IP address. Enter credentials for access to the mail service.
If SSL encrypted transmission is preferred, select its checkbox.

Click Add to complete the configuration.

4-3. Settings > User Management

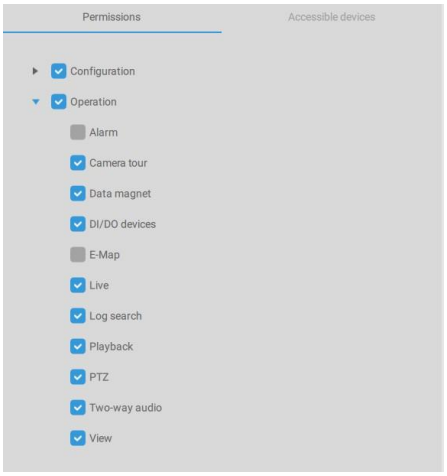
The User Add & Delete page allows you to create users with the permissions for different operational capabilities.

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

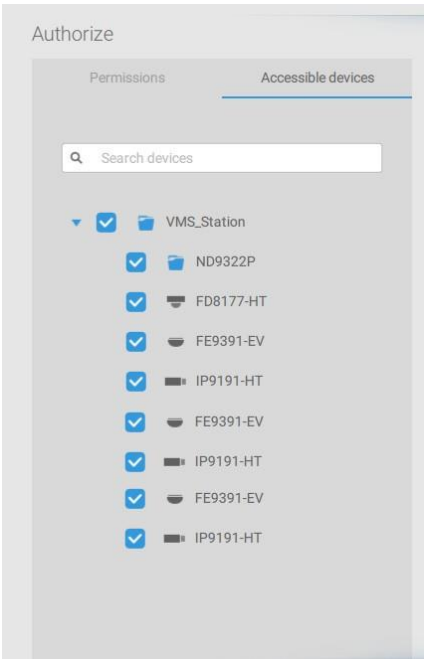


Use the Customize option to limit the authorized actions of a user.
In the Permissions tab, click the expand button  to unfold the Operation and Configuration menus. Select or deselect the checkboxes to

configure the user privileges. For example, you may not want a user to operate Alarm and E-Map. If so, deselect these checkboxes.



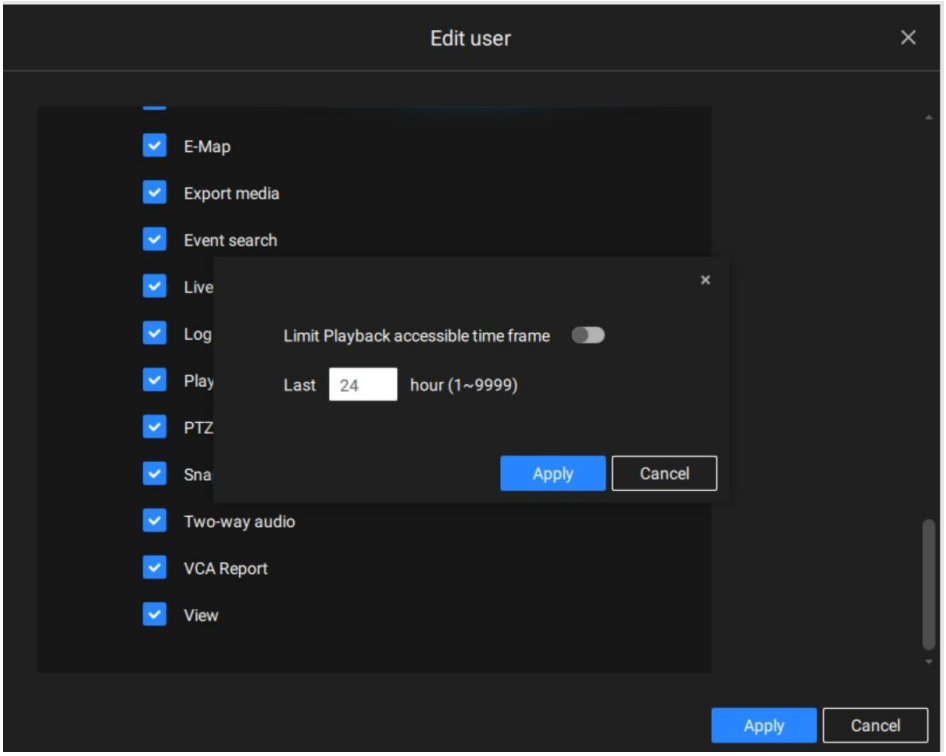
In the Accessible devices tab, click to select the cameras that a user can access. Some users may only need to access specific devices.



When done with the privilege settings, click Add to create a new user.

The new users will be listed under the Administrator's icon. Repeat the process to create more users.

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.



Add a New User Account - Windows AD Account

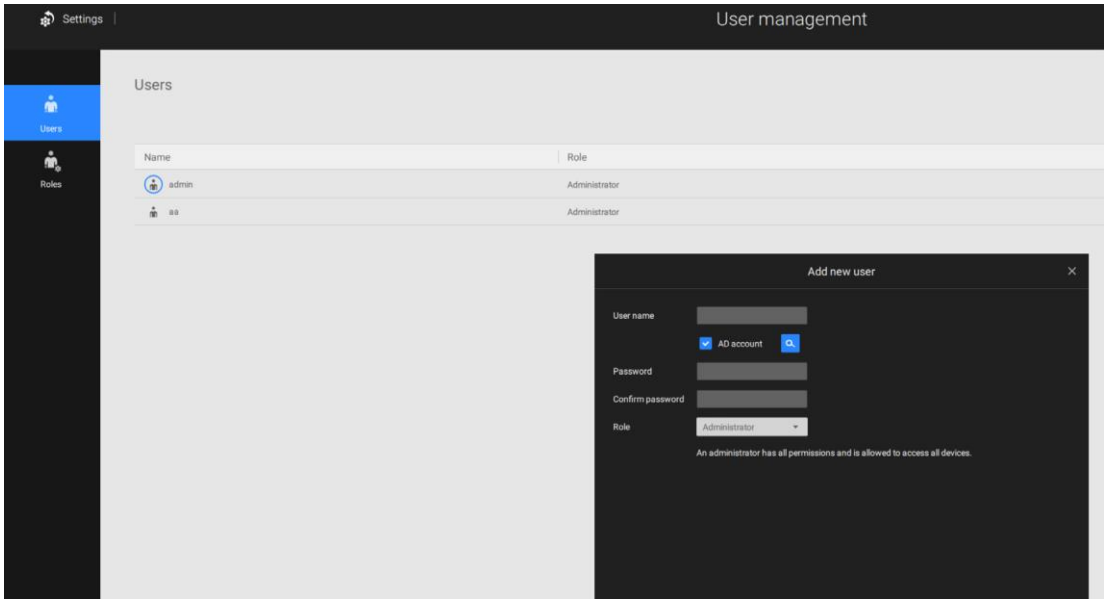
In an established, enterprise network environment, the support for Windows AD (Active Directory) infrastructure enables ease of integration using the credentials of existing users. Using the same AD authentication methodologies, you can configure the clients or users in an established network to access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

Note the following with Windows AD support:

1. If you install VSS server on a Windows XP machine with PostgreSQL server, the login using a Windows AD account will not work.
2. The VSS 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 VSS.
5. A User Group and its members configured in AD cannot be managed in VSS.
6. You cannot add an account having the same name as one you used to log in VSS.
7. There are 3 types of account for VSS: 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 VSS.
9. The userPrincipalName field of your Windows AD account should not be empty.

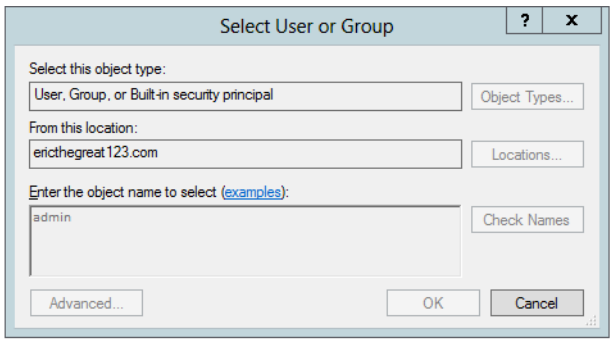
To add an existing AD user:

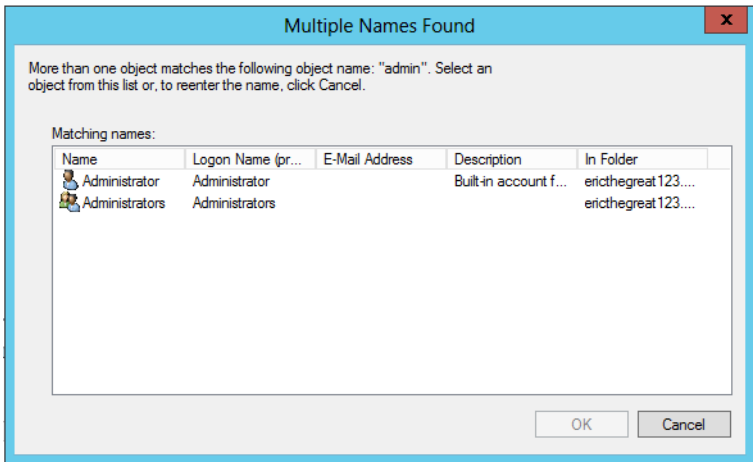
1. Select the AD account checkbox.



2. Click the Search button.

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





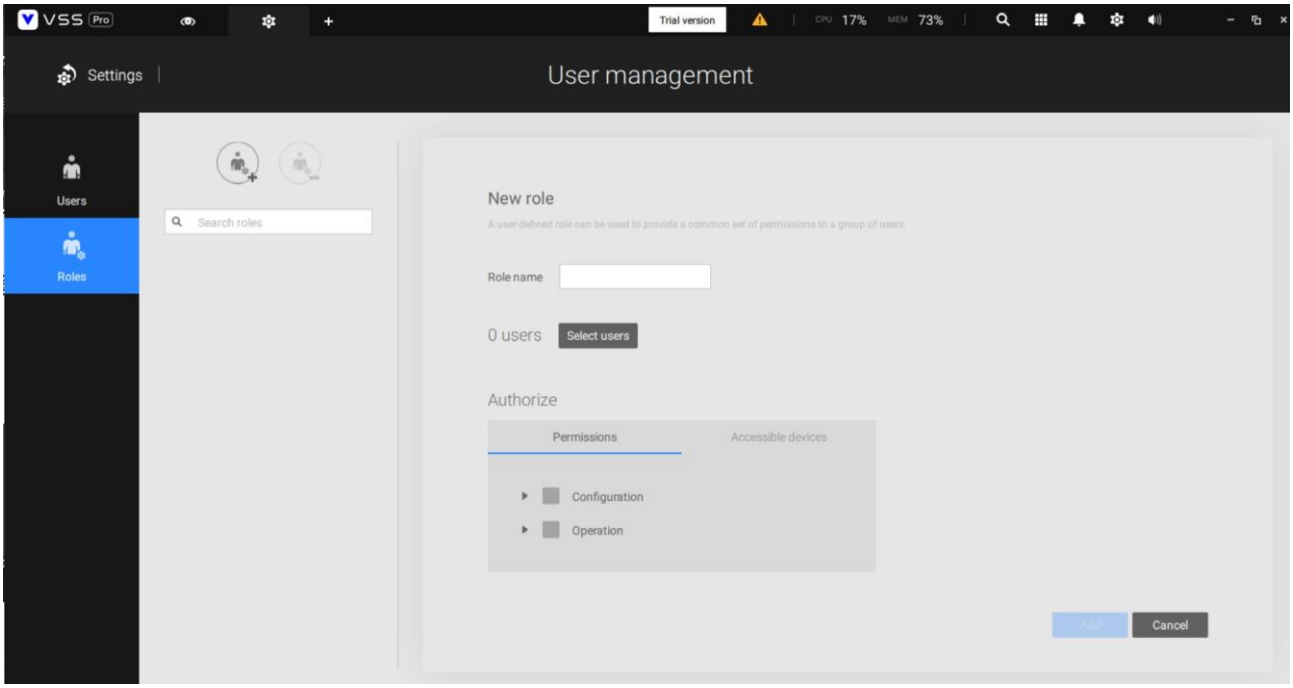
4. Enter the password twice for the AD user.

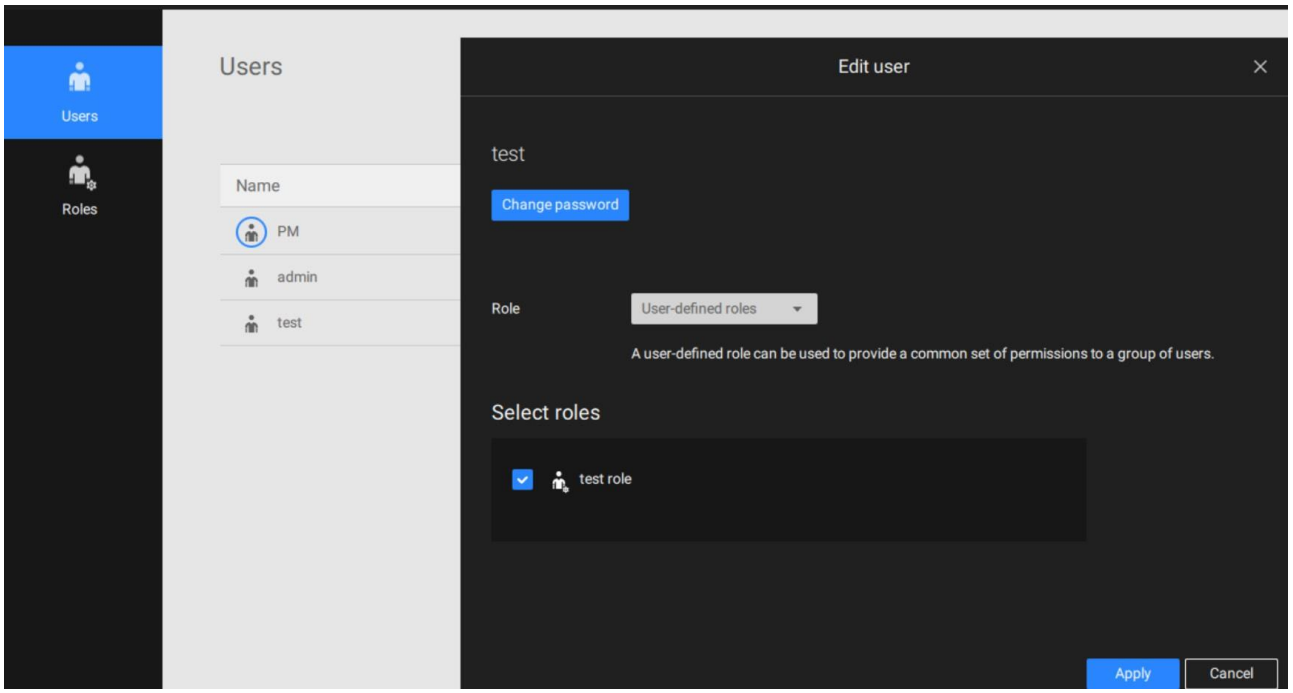
5. Select the privilege role for the user, configure his/her privilege settings as described above and then click Add.

User Roles

A user-defined role allows you to define a common set of permission for a group of users, reducing the setup time for different groups of users.

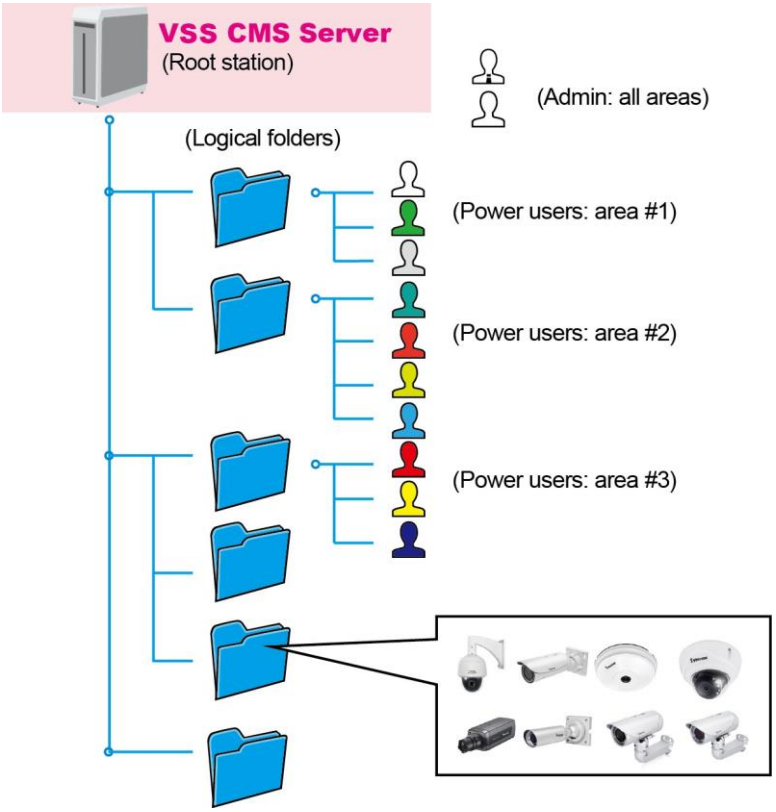
You can specify the role name in the first column. Also, you can select existing users for this new role. Note that once the users are selected for a new role, it will change its role and corresponding authorities. Each role can be assigned with the permissions and accessible devices like customized settings in user accounts. Users can select more than one role and have the unified settings for all roles' permissions.





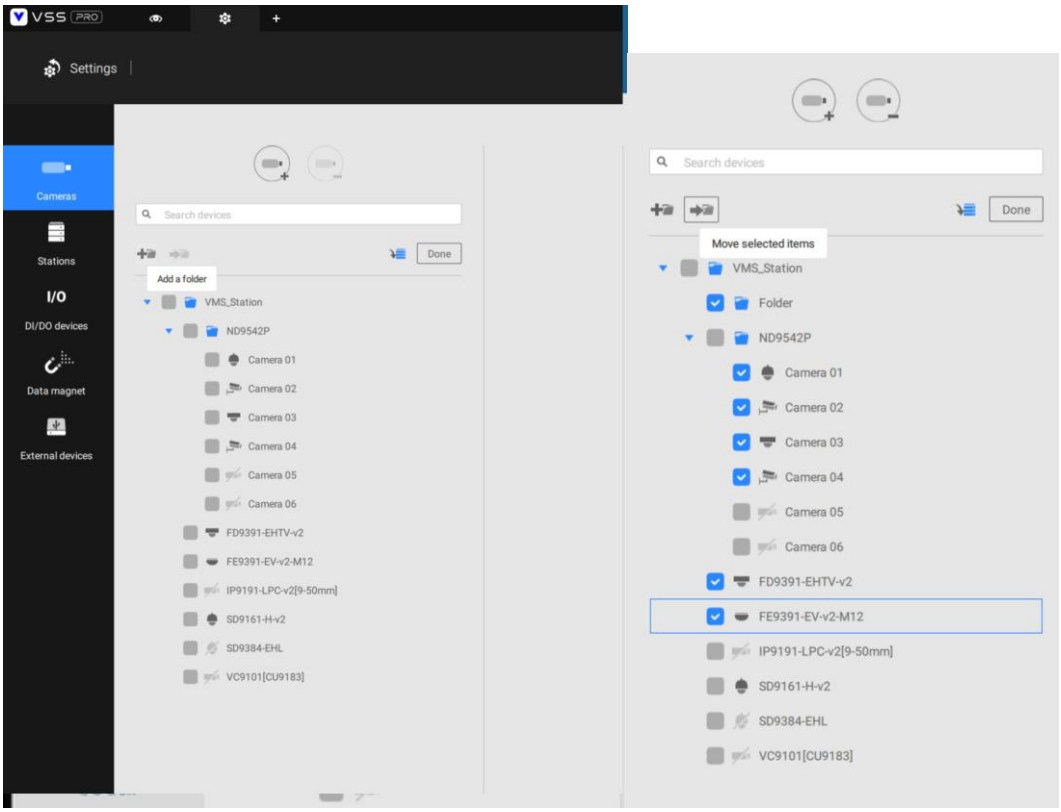
Logical Folders

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.

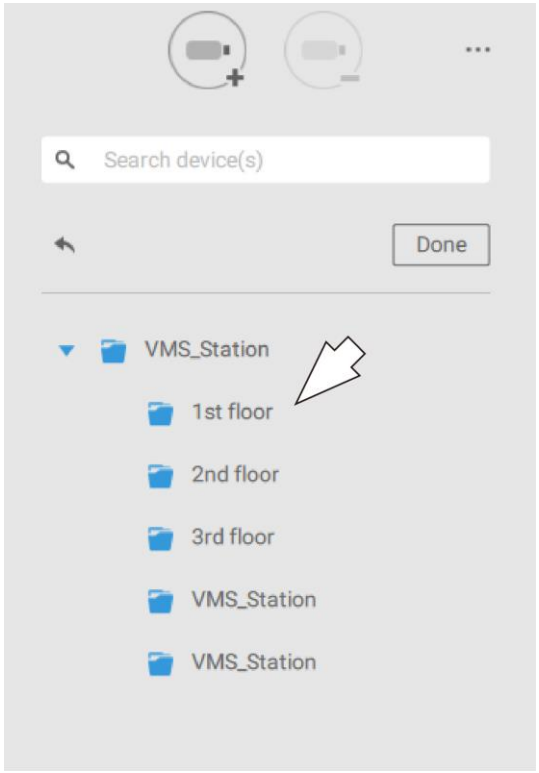


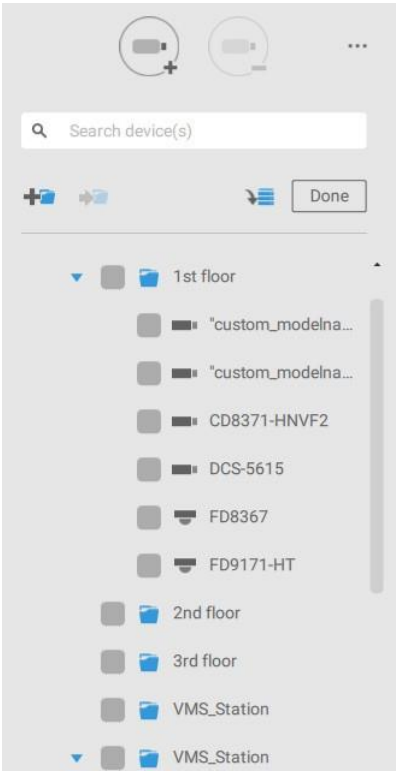
To create logical folders:

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.

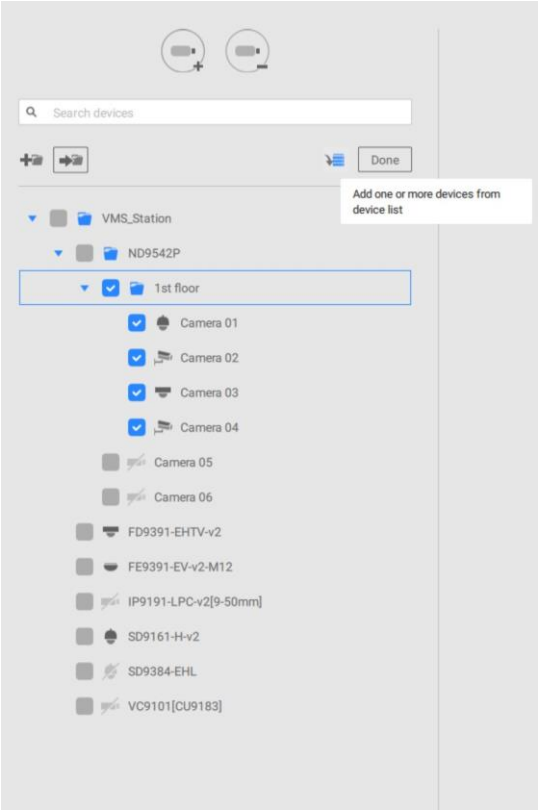


6. Select a logical folder to move the devices to. The selected devices will be listed under the logical folder you selected. Repeat the process to move cameras to each logical folder.

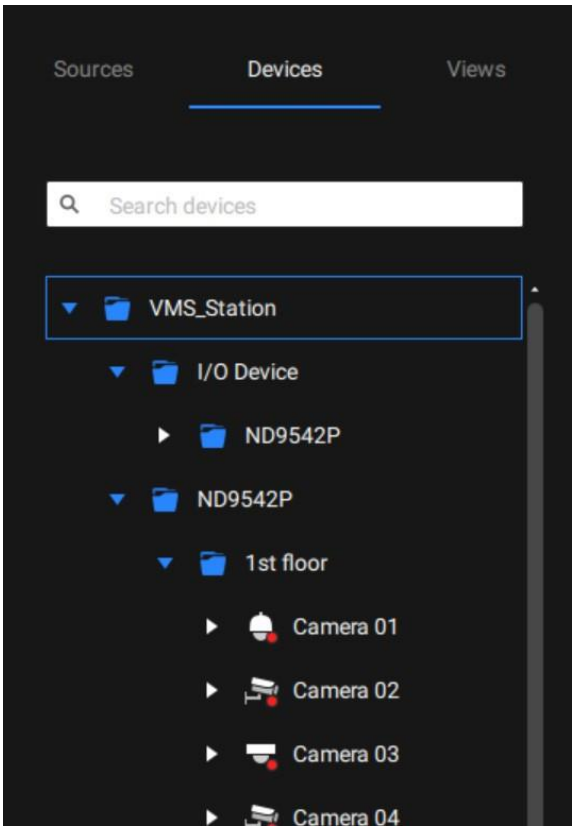




You can also use the add device button to select devices from the list and move them to a specific folder.



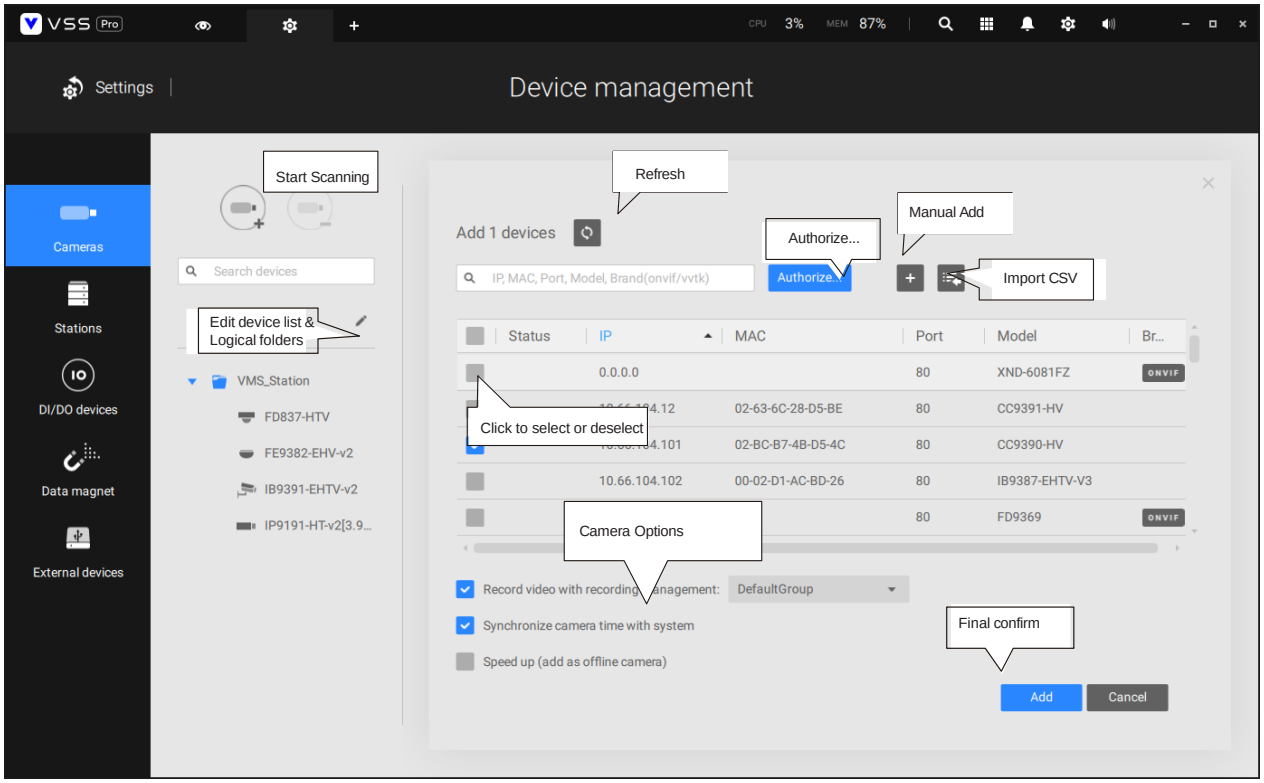
Return to live view, and you can see the configuration change takes effect.



4-4. Settings > 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 > Device > Cameras.

Below are the locations of the functions for adding devices (after clicking) to the VSS server.



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

For cameras outside the local network, you can manually enter its IP address, or use a pre-configured device list to automatically introduce new devices.

If all devices come with the same credentials, you can select these devices and click Authorize to enter the credentials.

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

Speed up (add as offline cameras): Normally, you should have all the credentials for 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 applies 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, VSS will attempt to connect with them.

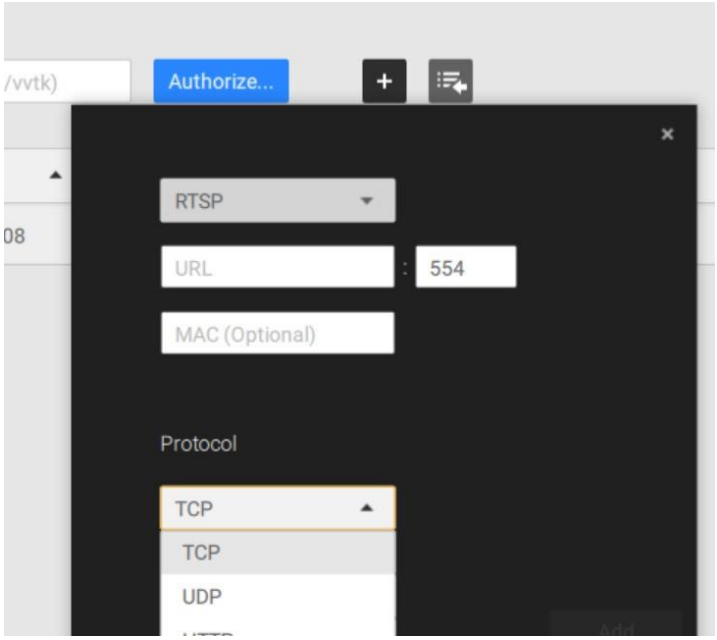
- Retrieve RTSP streaming on specific port: The default port for RTSP streaming is 554. If you want to change this port, please check this item and fill in a desired port number.

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**."

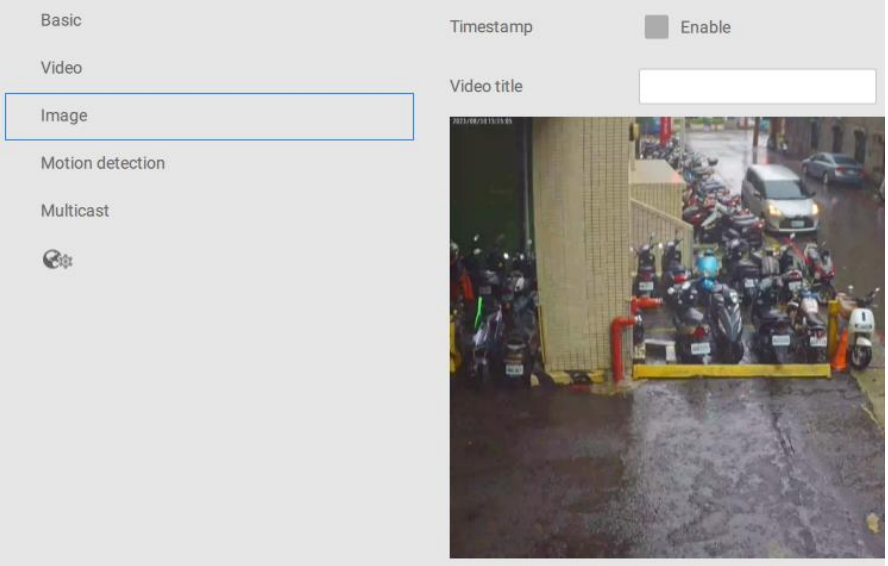


2. Enter the camera's IP address.
3. Enter the camera's MAC address as printed on the camera label, or one found by the Shepherd utility.
4. Enter "554" in the Configuration port.
5. Enter "live.sdp" in the URL field, as this is part of the original RTSP streaming command: "rtsp://172.18.204.58:554/live.sdp". If streaming stream #2, enter live2.sdp.
6. Select a preferred protocol.

   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.

7. For administrators who need to synchronize device time with an NTP server, he can deselect the "Synchronize camera time with system" checkbox.

11. If you click a specific camera, you will see five tabs: Basic, Video, Image, Motion detection, and multicast (the last two tabs may be empty depending on camera models):



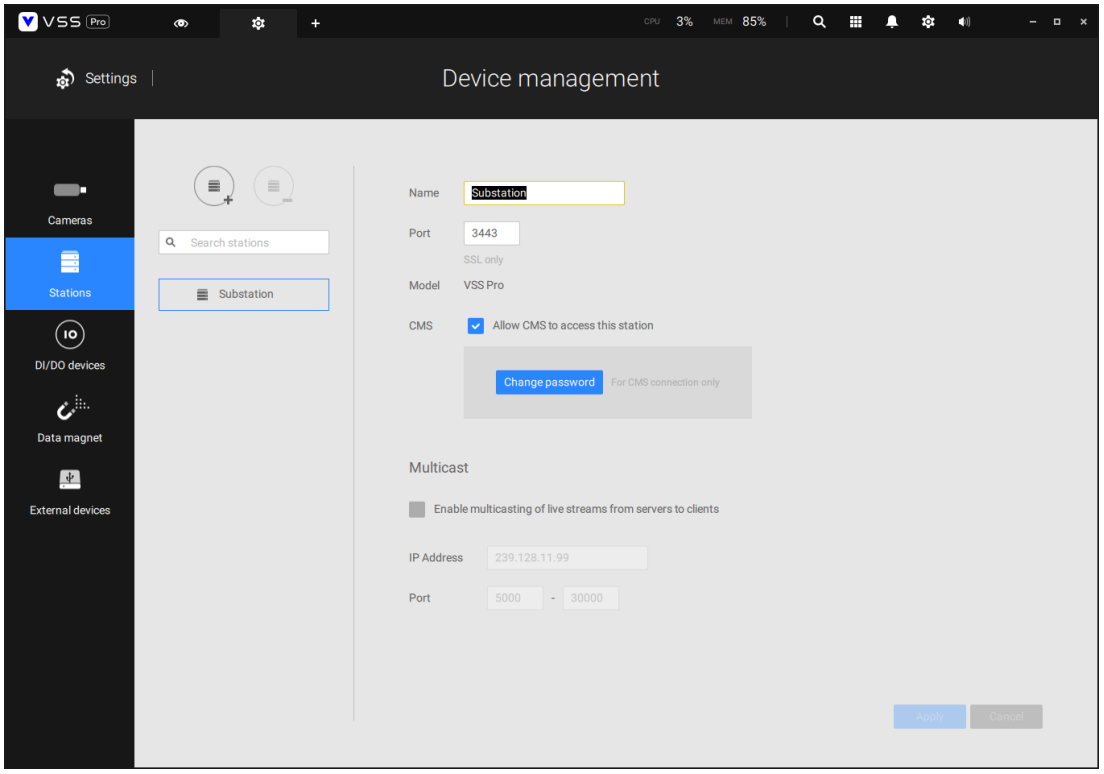
12. Basic: shows the fundamental information including camera name, addresses of IP, port & MAC, brand, and protocol
13. Video: provides options for video quality settings such as type, frame size, and frame rate
14. Image: selects whether to enable timestamp and add a video title name
15. Motion detection: selects whether to enable motion detection in your video and the detection sensitivity
16. Multicast: selects whether to enable server-side multicast streaming
17. More settings on the Web: provides the browser-based UI for other settings
18. PTZ Settings (Optional for PTZ camera):
19. PTZ default: enable or disable the PTZ control on live view.
20. PTZ operation mode: select a control method for click and drag on the live view
21. Track mode: select the tracking function on live view, for cameras that support smart tracking or smart tracking advanced, please pre-configure the related setting on the camera web first and refer to the Smart Tracking User Guide for details
22. Enable track if the camera idles for xx seconds. It is recommended to enable this function while PTZ has tracking tasks in daily operation. Note that manual PTZ control always has a higher priority and will interrupt the tracking.
23. Note that if the camera is connected under the ND NVR substation, some functions may not be configurable.

4-5. Settings > Device > Stations

The VSS allows a deployment consisting of multiple VSS instances at different locations. A VSS server can be selected as the CMS (Central Management Server) to manage sub-stations in a hierarchical structure.

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

1. Open the VSS 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 VSS server and substations.

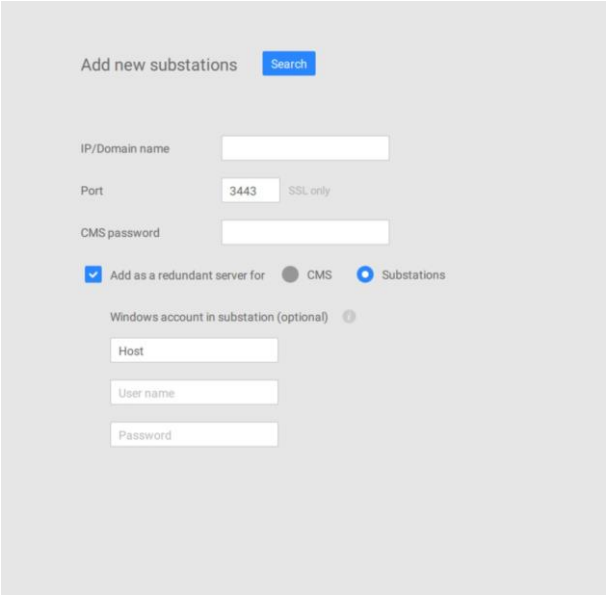


6. Click the Apply button.

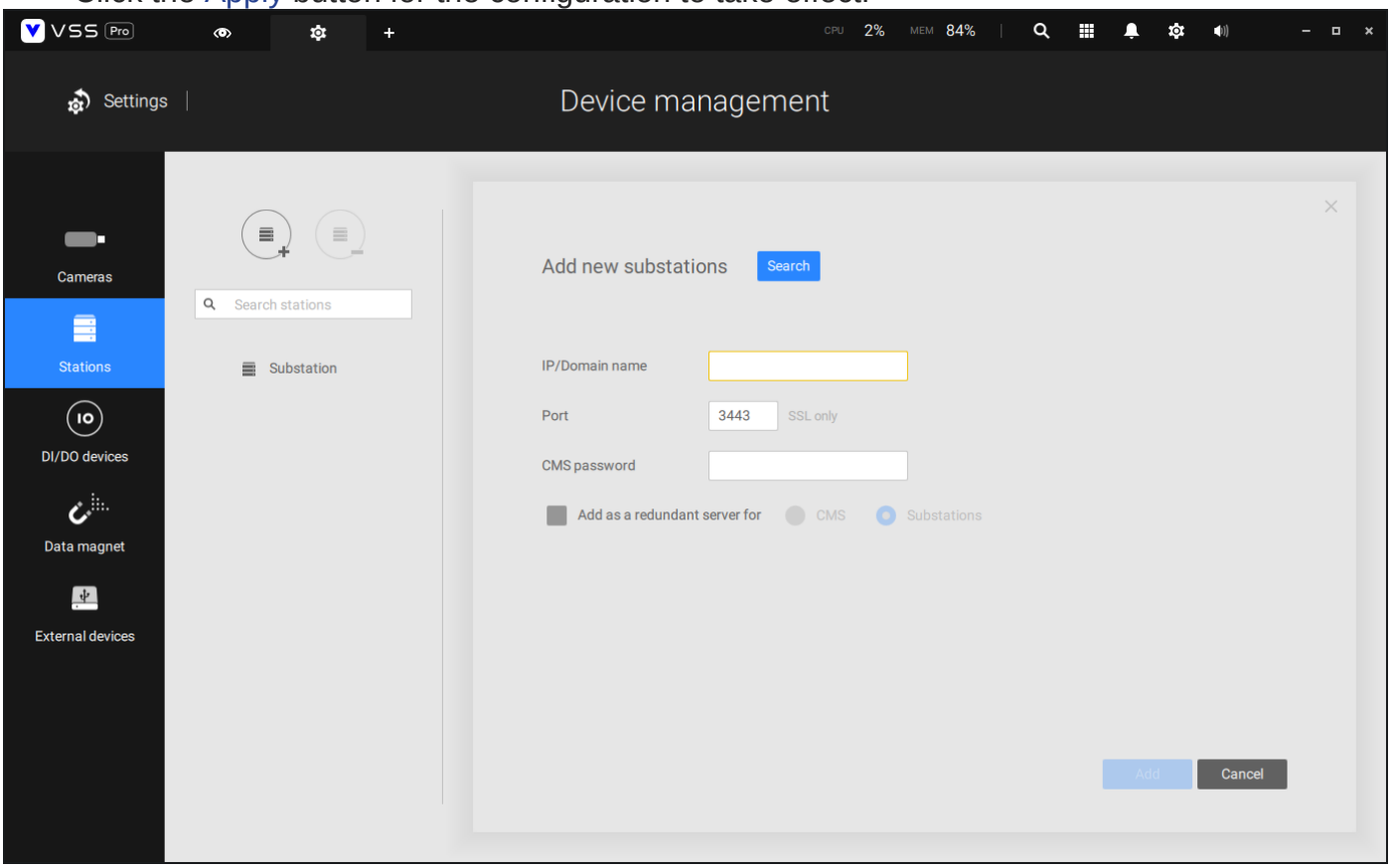
7. Open the VSS client on the server chosen as the CMS.

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

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



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.

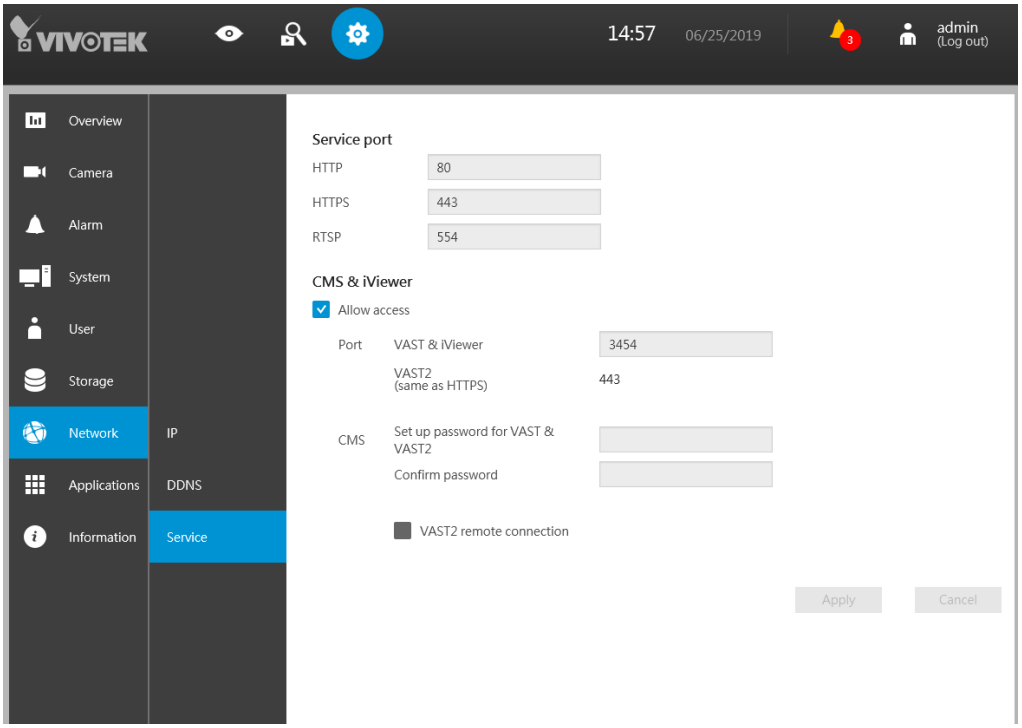


The substations and their subordinate devices should be immediately listed under the CMS station. You can create separate views to place the substations' cameras.

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

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

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



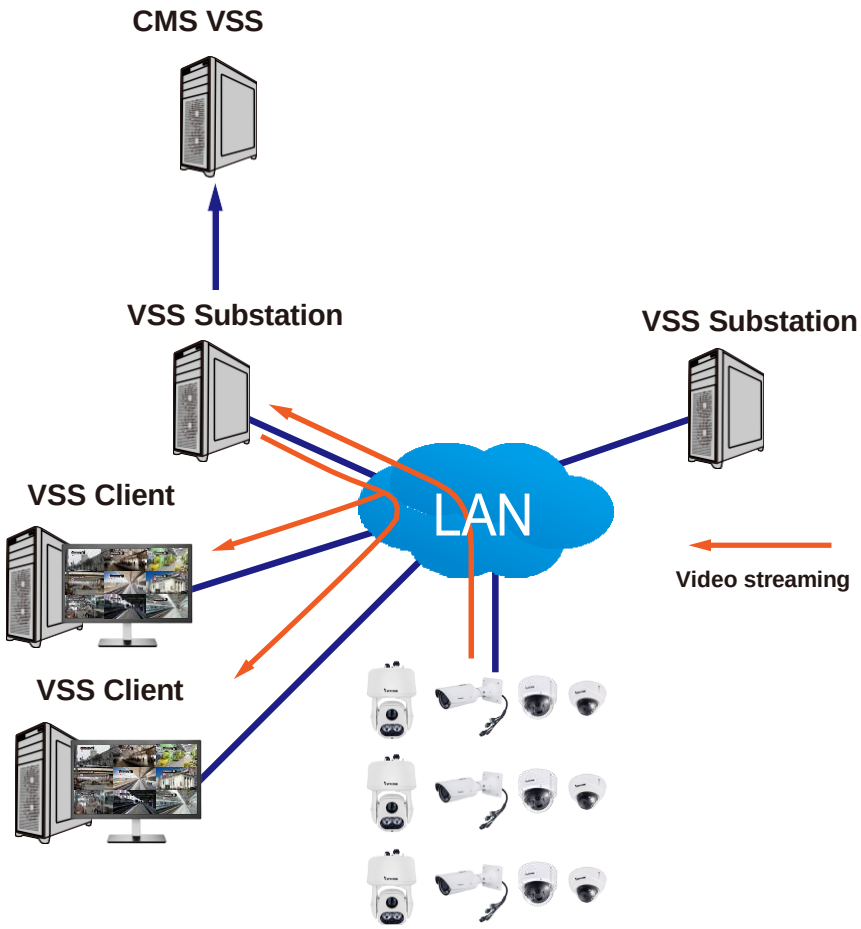
Multicasting

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

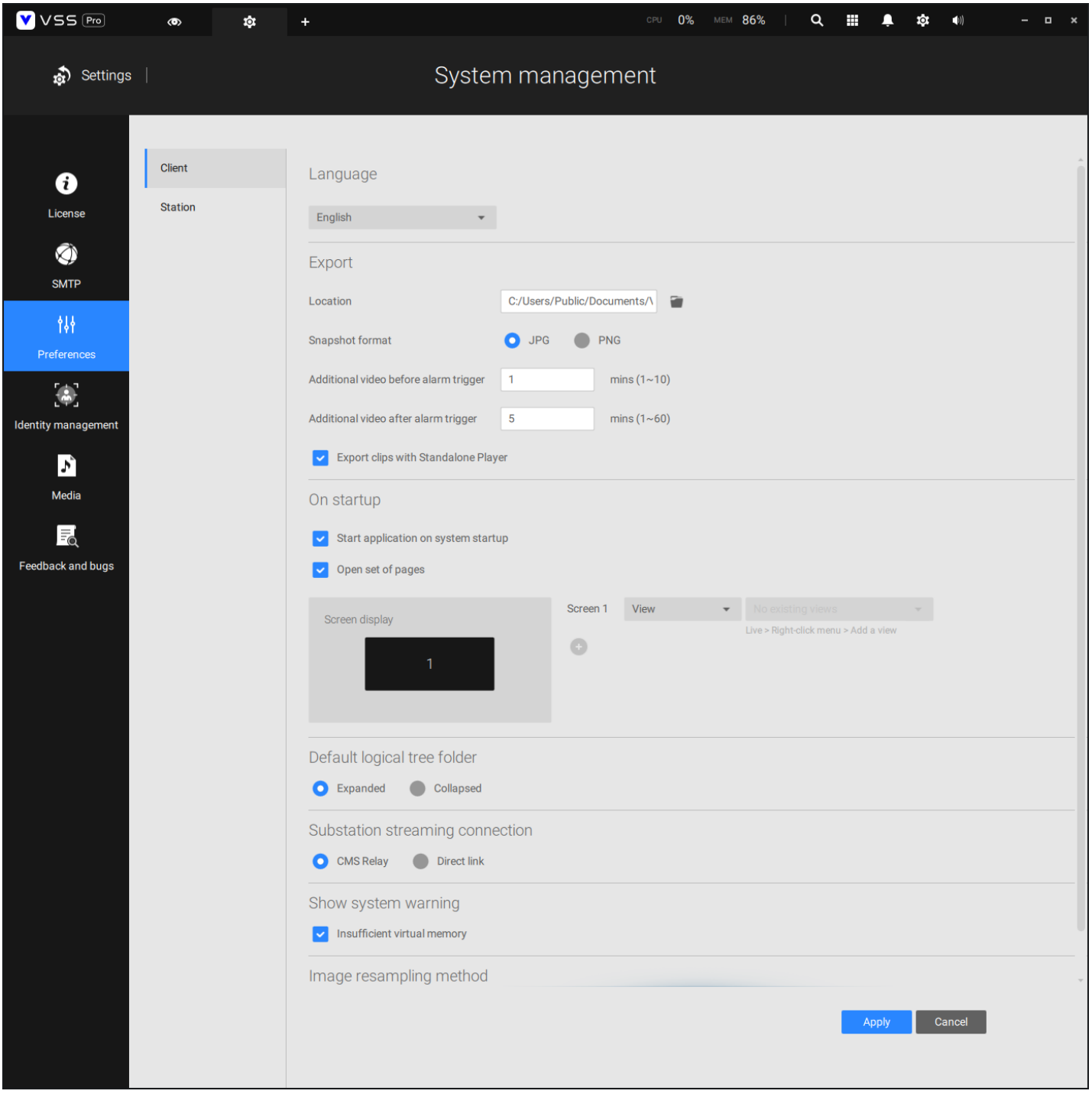
Multicasting should be enabled on a VSS server and also on individual cameras.

There are prerequisites:
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 VSS 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.

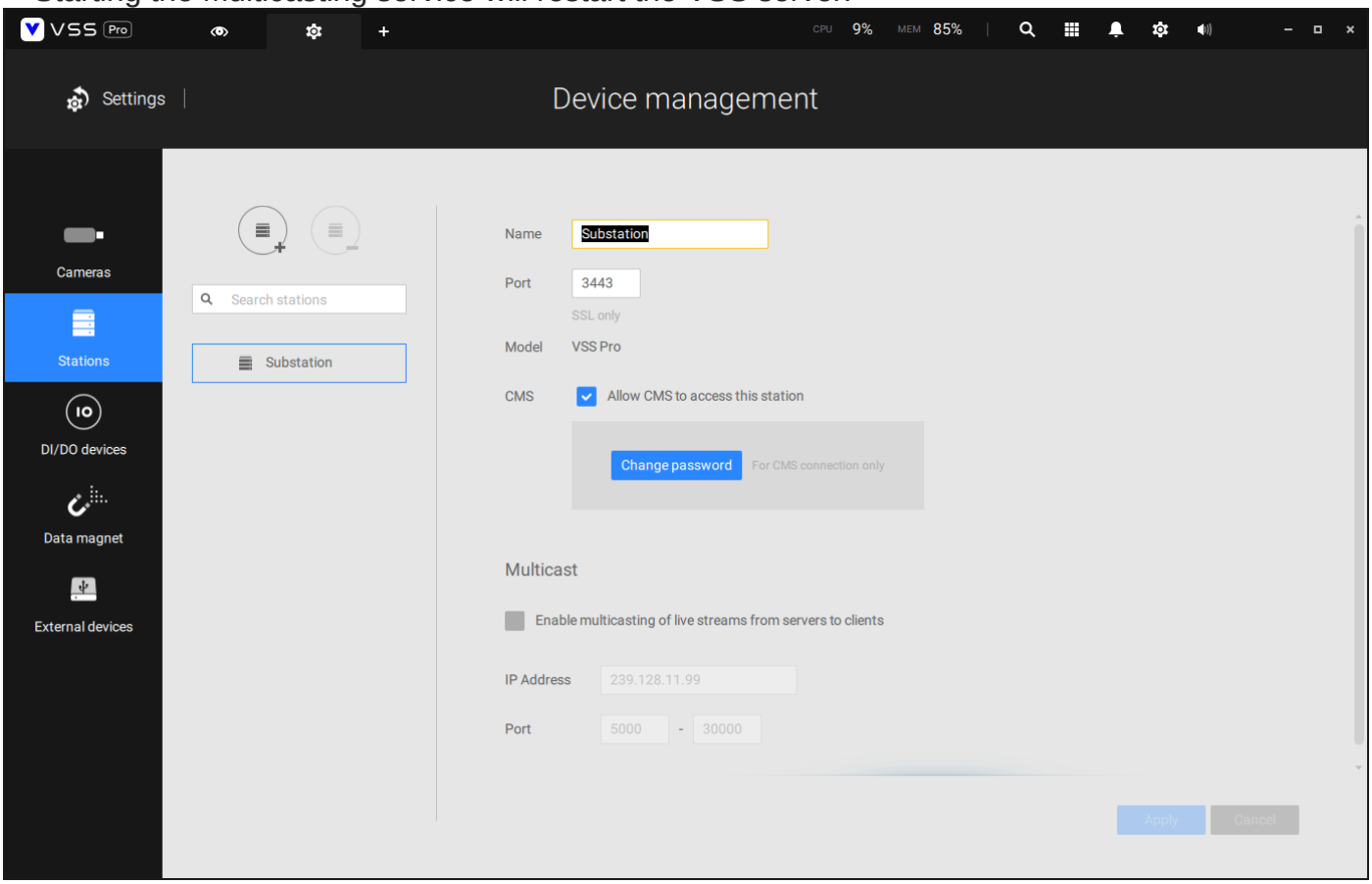


* To enable multicasting, your network infrastructure must support the IP multicasting standard IGMP (Internet Group Management Protocol). Your server and clients should be on the same network segment.
* Multicasting is only possible for live streams, not applicable to the recorded video or audio.
* Multicast streams are not encrypted, even if the 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 VSS server:

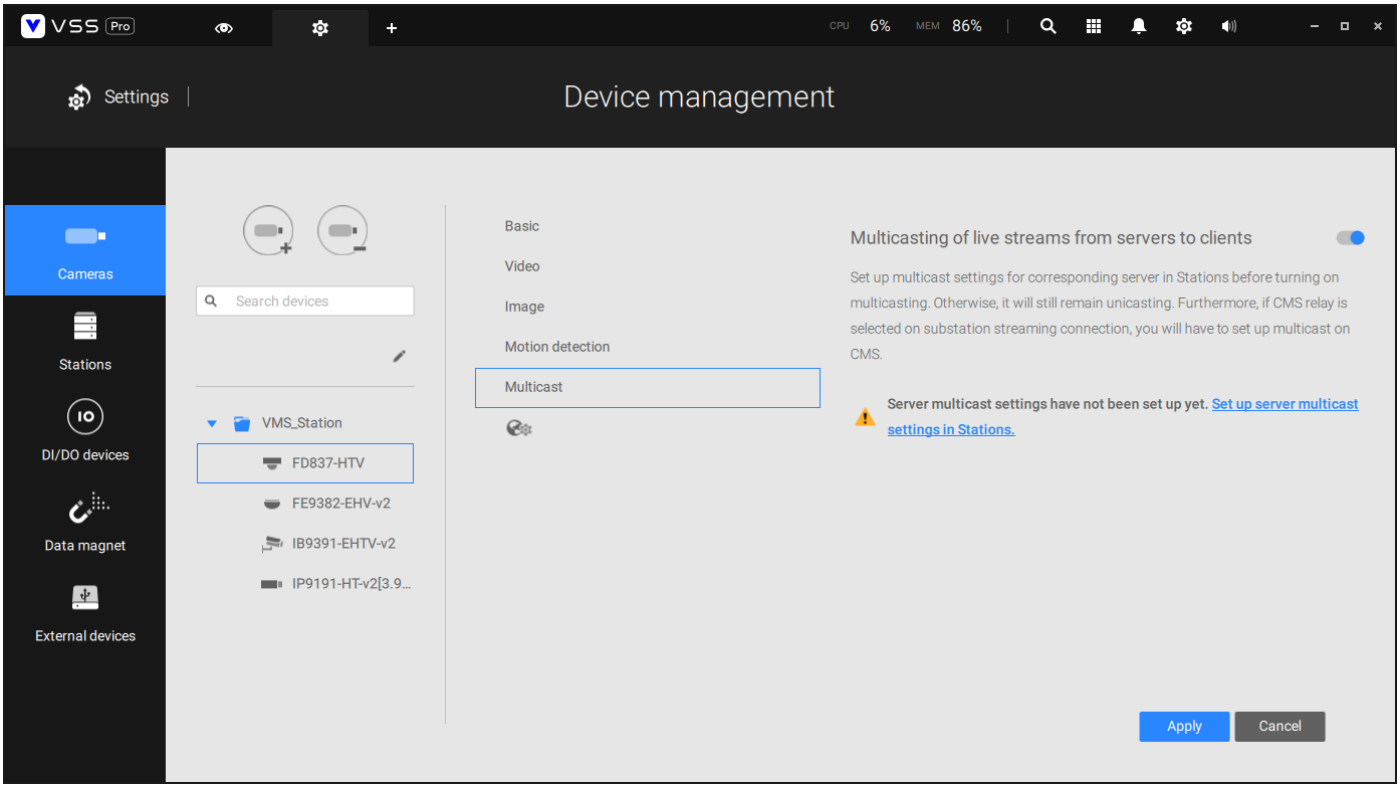
1. Enter Settings > Device > Stations.
2. Single-click to select a server for which you want to enable the Multicasting.
3. Click the checkbox to enable the configuration and enter the multicast address.
4. Click the **Apply** button.

Starting the Multicasting service will restart the VSS server.



To enable Multicasting on a camera:

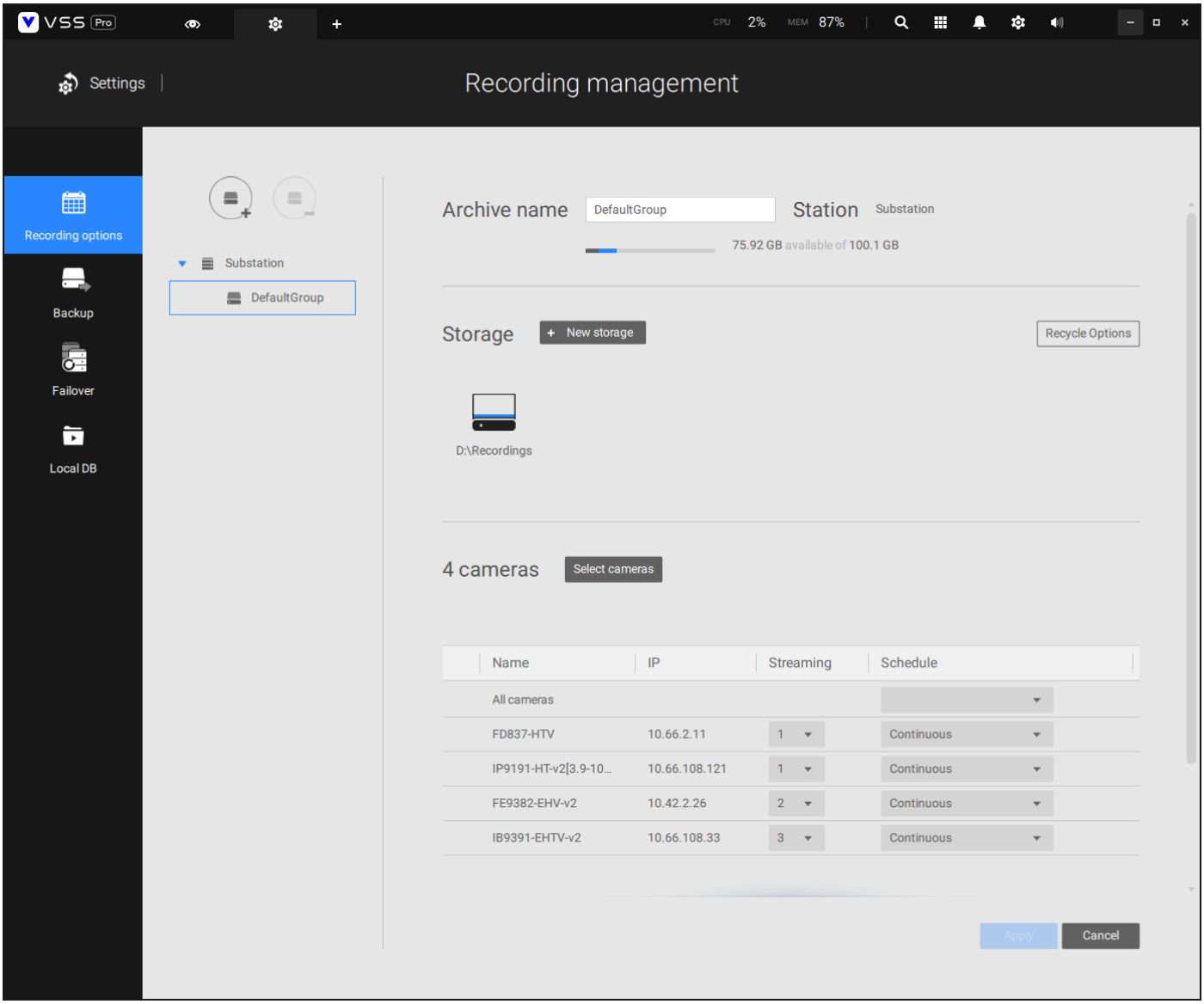
1. Enter Settings > Device > Cameras.
2. Single-click to select a camera for which you want to enable the Multicasting.
3. Click to select the Multicast tab.
4. Click the Multicasting slide button.
5. Click the **Apply** button.



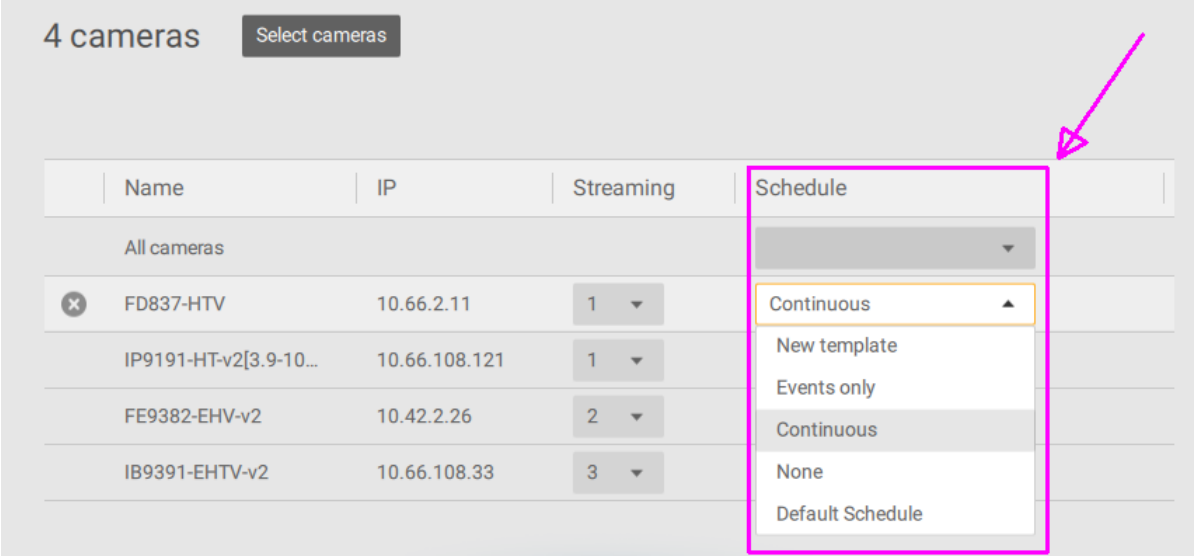
4-6. Settings > Recording > Recording Options

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

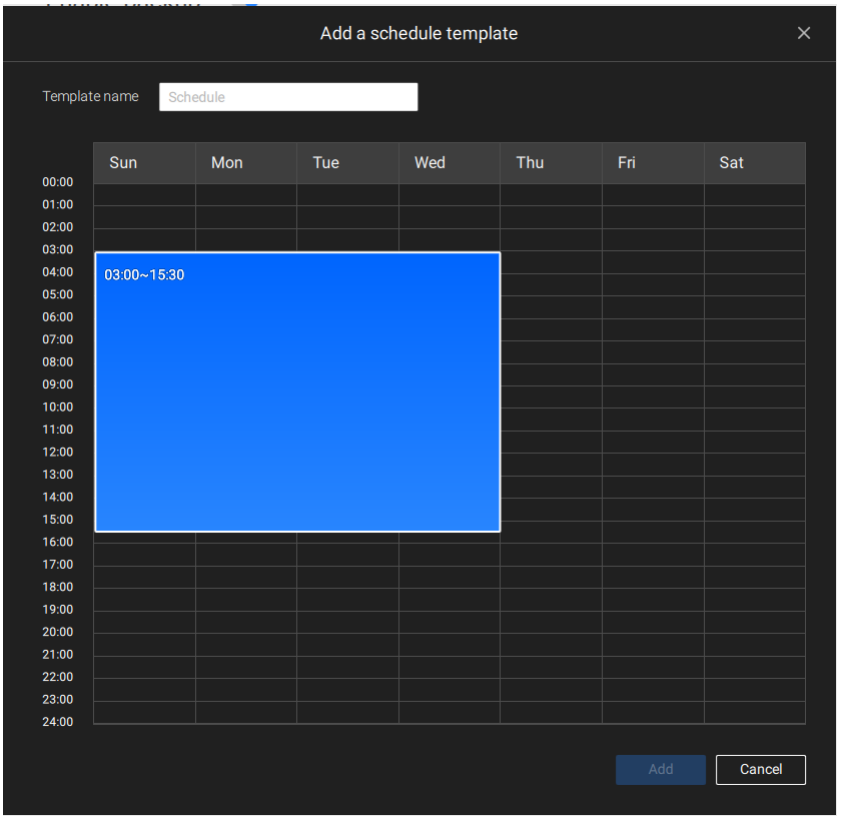
You can configure recording schedules or select the storage options, including the configuration of an external NAS storage. You can designate a recording folder of your choice.



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 button.



Click and hold down on the time cells, and drag the mouse to include the time span of your preference. 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.

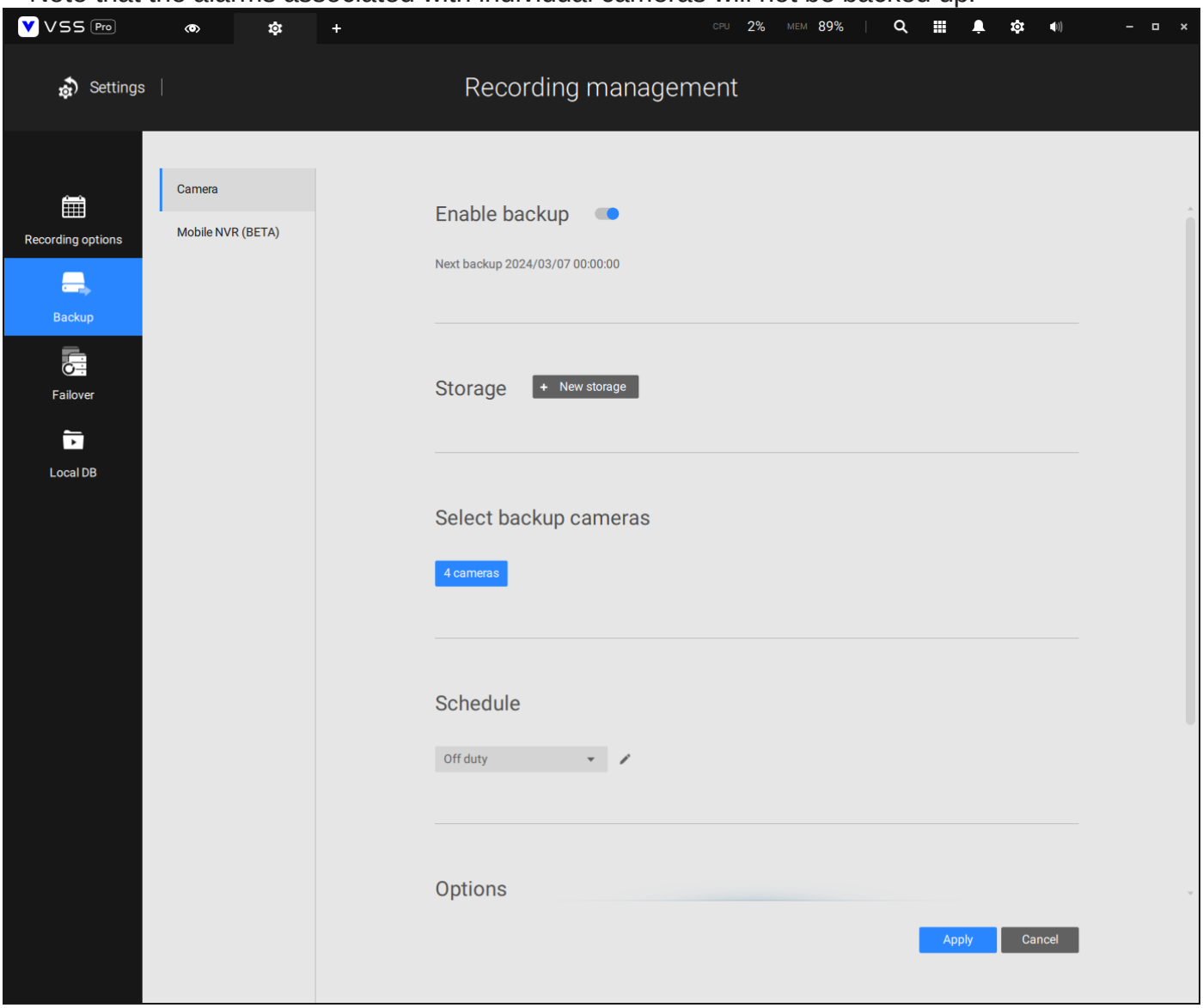
The same configuration window applies to both the Schedule template and the customize schedule windows.

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

4-7. Settings > Recording > Backup

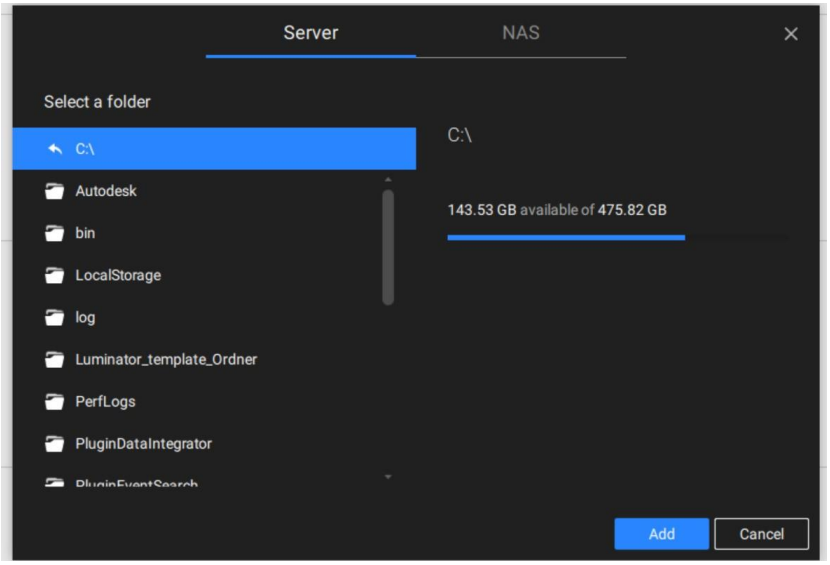
The Backup function allows you to regularly back up the video recordings of one or multiple cameras to local hard disks or a Network Attached Storage device. Currently, the VSS server does not support backup to external storage devices such as a storage devices connected via Fiber Channel. VSS supports backup to an external storage attached through a USB 3.0 connection.

Note that the alarms associated with individual cameras will not be backed up.

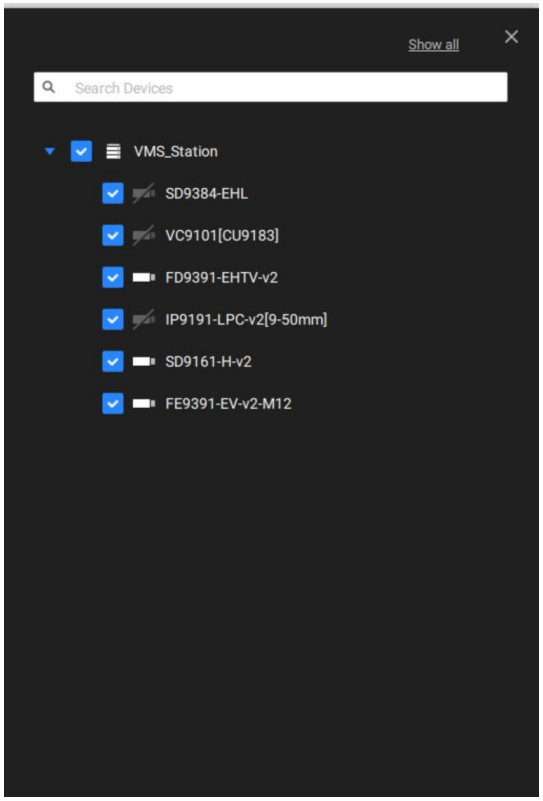


To enable a backup schedule:

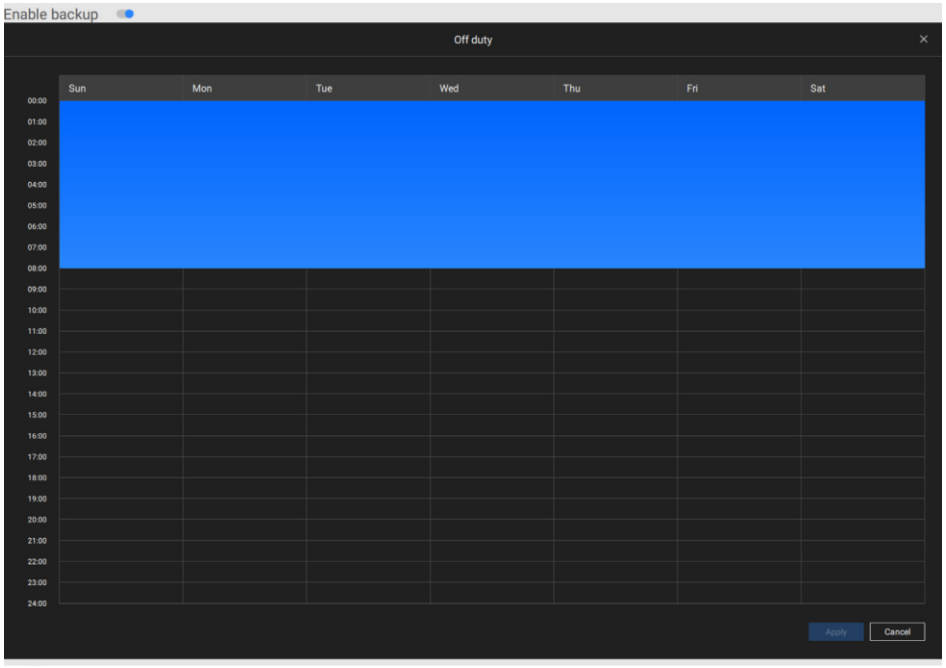
1. Enable the backup by selecting the "Enable backup" slide switch.
2. Click to add New storage. A configuration window will prompt showing all accessible storage. Click the NAS tab to enable access to a network share.



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

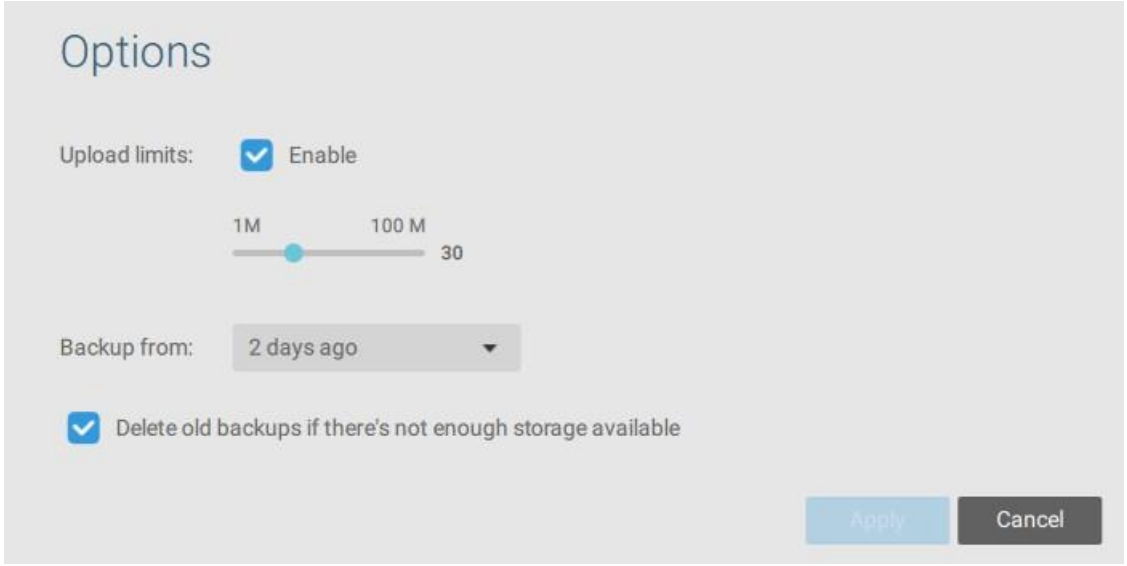


4. Select or configure a new schedule template for the backup process to take place. You can select a time when the network load is low, such as the off-office hours, to avoid network congestions.



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

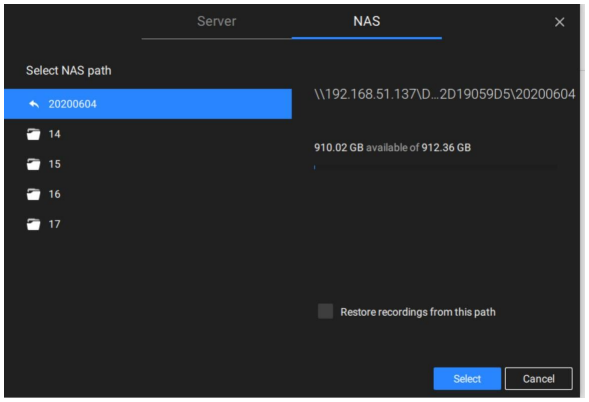
   You can select the extension of time, such as starting from how many days ago, of your backup task. You can select to remove old backups when you run short of storage volume.



Storage

By default, VSS 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.



Select storage volumes each by a single click.

Click **Ready to use** to continue.

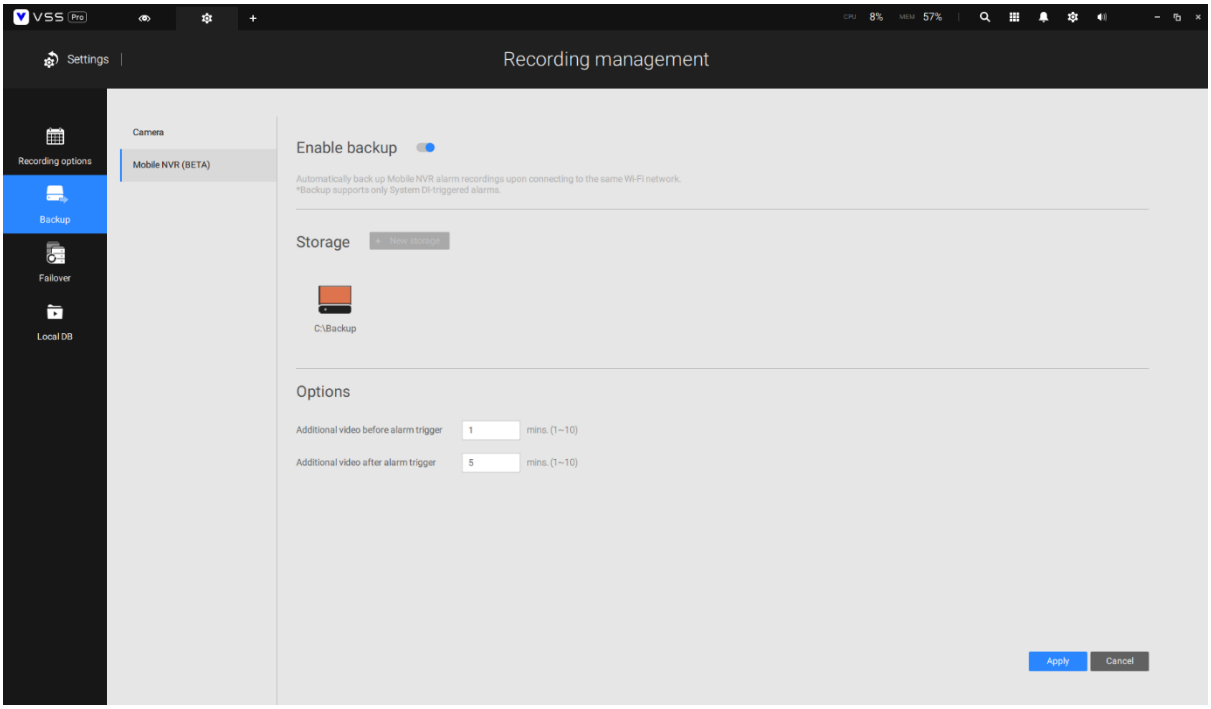
Mobile NVR Wi-Fi Backup (BETA)

This feature allows Mobile NVRs to initiate a backup of specific Alarm recordings upon arriving at a location with a WiFi Access Point (AP) connected to the same domain as the VSS CMS server. Only the System DI-triggered alarm is supported in the current edition.

Here are the setup steps:

To set up VSS Server:

1. Add the Mobile NVR to the VSS Server as a substation.
2. Navigate to Settings -> Recording -> Backup -> Mobile NVR. Enable backup for Mobile NVR.
3. Choose the storage path for the recordings to be backed up.
4. Set the duration for recording backups before and after the occurrence of an alarm trigger.



To set up Mobile NVR:

1. Set up the WiFi connection on the Mobile NVR to connect to WiFi Access Points.
2. Set up Alarm configurations on the Mobile NVR. Specify the System DI (Digital Input) as the trigger for the Alarm. Specify Video recording as an action for Alarm, including which cameras should start recording.

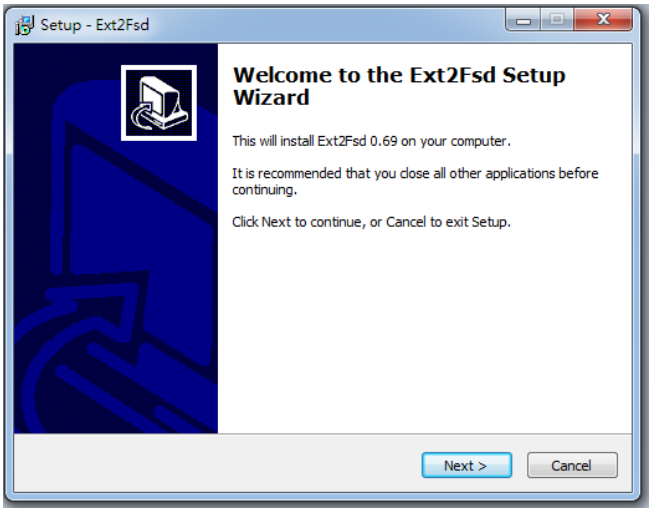
Once these steps are completed, when the Mobile NVR connects to the WiFi AP in the same domain as the VSS CMS server, the CMS server will establish a connection to the Mobile NVR and transfer the System DI-triggered alarms recording to the VSS server for backup.

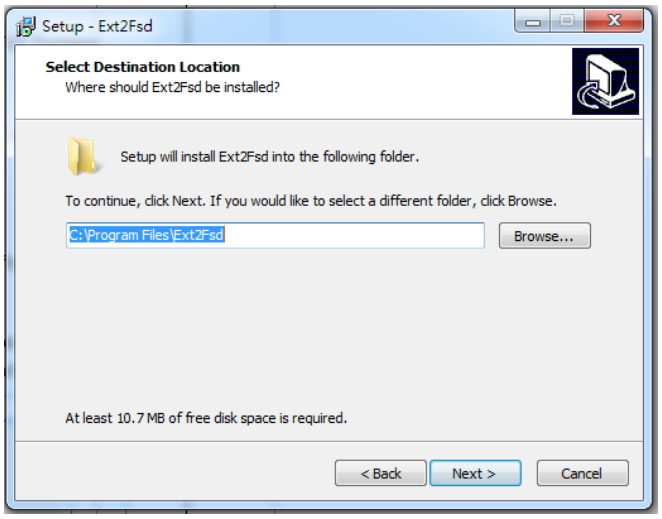
4-8. Settings > Recording > Local DB

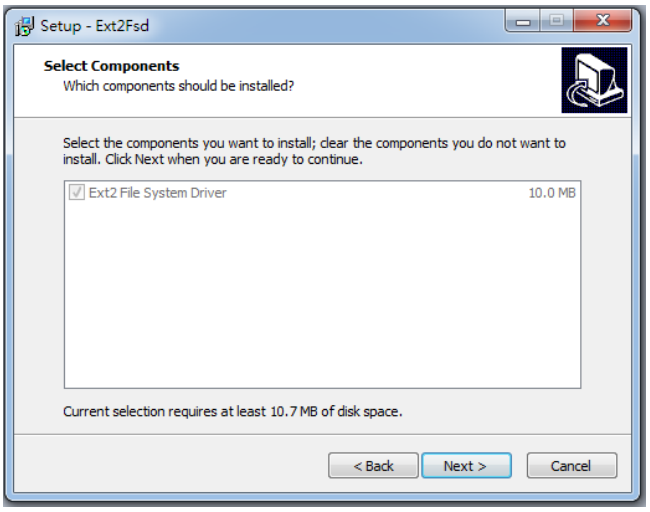
Since some of VIVOTEK's NVRs run on Linux, you have to install the Ext2 File System Driver for Windows to access the recording files from a NVR hard disk.

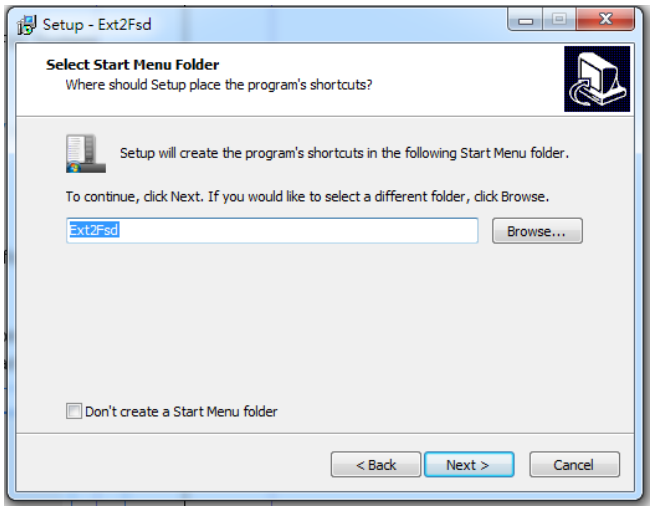
The file system driver can be found here: https://sourceforge.net/projects/ext2fsd/?source=typ_redirect

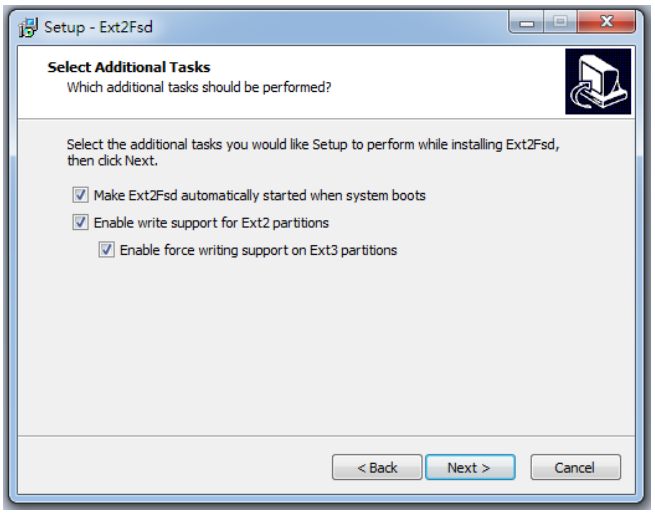
Run and install the Ext2fsd-0.xx.exe. Follow the onscreen instructions to complete the installation.

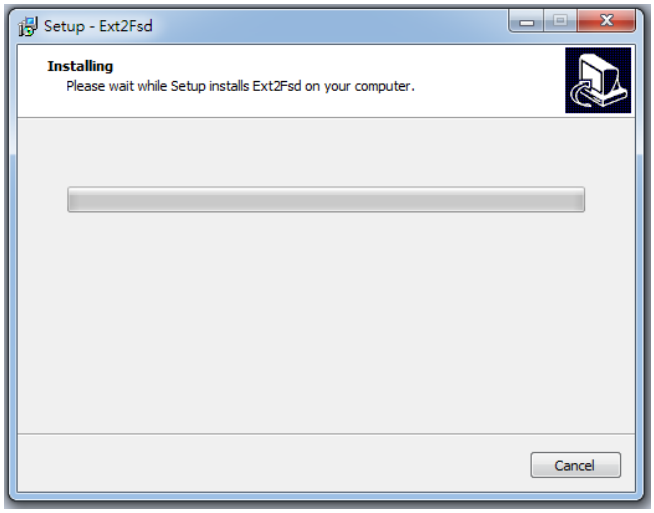


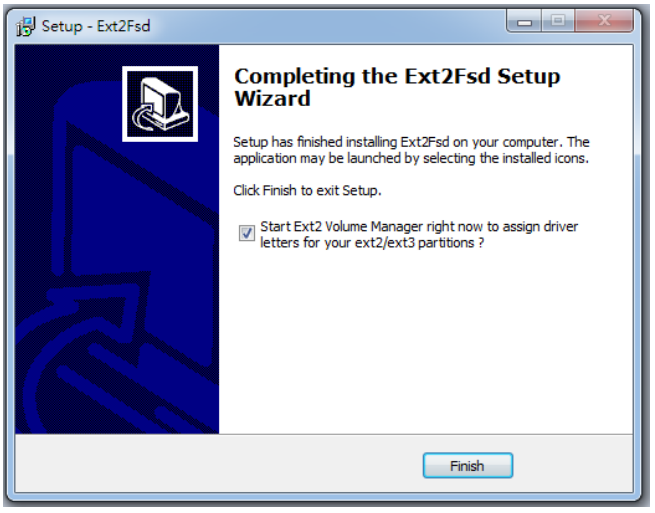


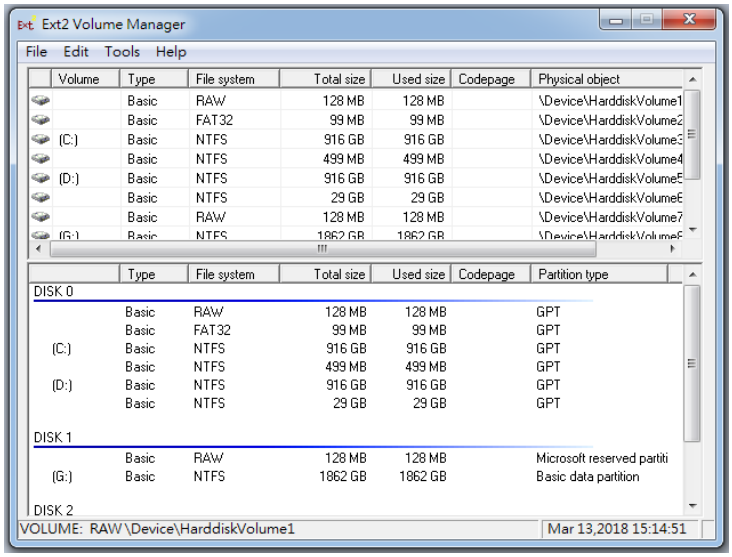



Setup - Ext2Fsd
Select Start Menu Folder
Where should Setup place the program's shortcuts?
Setup will create the program's shortcuts in the following Start Menu folder.
To continue, click Next. If you would like to select a different folder, click Browse.
Ext2Fsd
Browse...
Don't create a Start Menu folder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

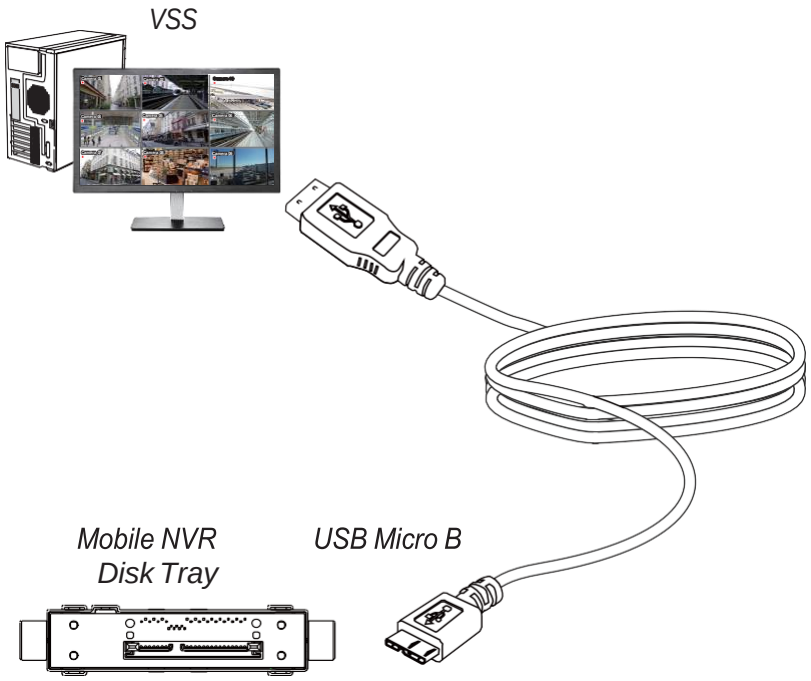

Setup - Ext2Fsd
Select Additional Tasks
Which additional tasks should be performed?
Select the additional tasks you would like Setup to perform while installing Ext2Fsd, then click Next.
Make Ext2Fsd automatically started when system boots
Enable write support for Ext2 partitions
Enable force writing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


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

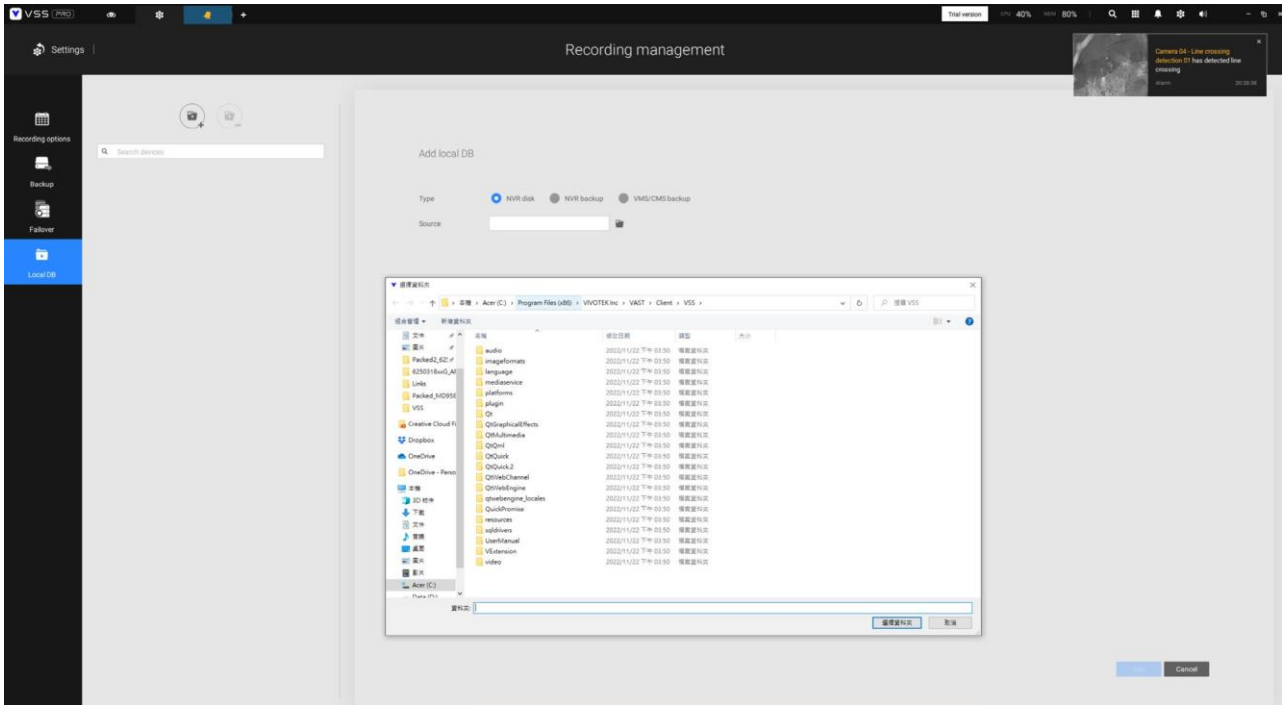

Setup - Ext2Fsd
Completing the Ext2Fsd Setup Wizard
Setup has finished installing Ext2Fsd on your computer. The application may be launched by selecting the installed icons.
Click Finish to exit Setup.
Start Ext2 Volume Manager right now to assign driver letters for your ext2/ext3 partitions ?
Finish


Ext2 Volume Manager
File Edit Tools Help
Volume Type File system Total size Used size Codepage Physical object
Basic RAW 128 MB 128 MB \Device\HarddiskVolume1
Basic FAT32 99 MB 99 MB \Device\HarddiskVolume2
(C:) Basic NTFS 916 GB 916 GB \Device\HarddiskVolume3
Basic NTFS 499 MB 499 MB \Device\HarddiskVolume4
(D:) Basic NTFS 916 GB 916 GB \Device\HarddiskVolume5
Basic NTFS 29 GB 29 GB \Device\HarddiskVolume6
Basic RAW 128 MB 128 MB \Device\HarddiskVolume7
Type File system Total size Used size Codepage Partition type
DISK 0
Basic RAW 128 MB 128 MB GPT
Basic FAT32 99 MB 99 MB GPT
(C:) Basic NTFS 916 GB 916 GB GPT
Basic NTFS 499 MB 499 MB GPT
(D:) Basic NTFS 916 GB 916 GB GPT
Basic NTFS 29 GB 29 GB GPT
DISK 1
Basic RAW 128 MB 128 MB Microsoft reserved partiti
(G:) Basic NTFS 1862 GB 1862 GB Basic data partition
DISK 2
VOLUME: RAW \Device\HarddiskVolume1
Mar 13,2018 15:14:51

1. Remove the disk tray box from a mobile NVR.
2. Connect the disk tray box to your VSS server using a USB 3.0 type A to Micro B cable.

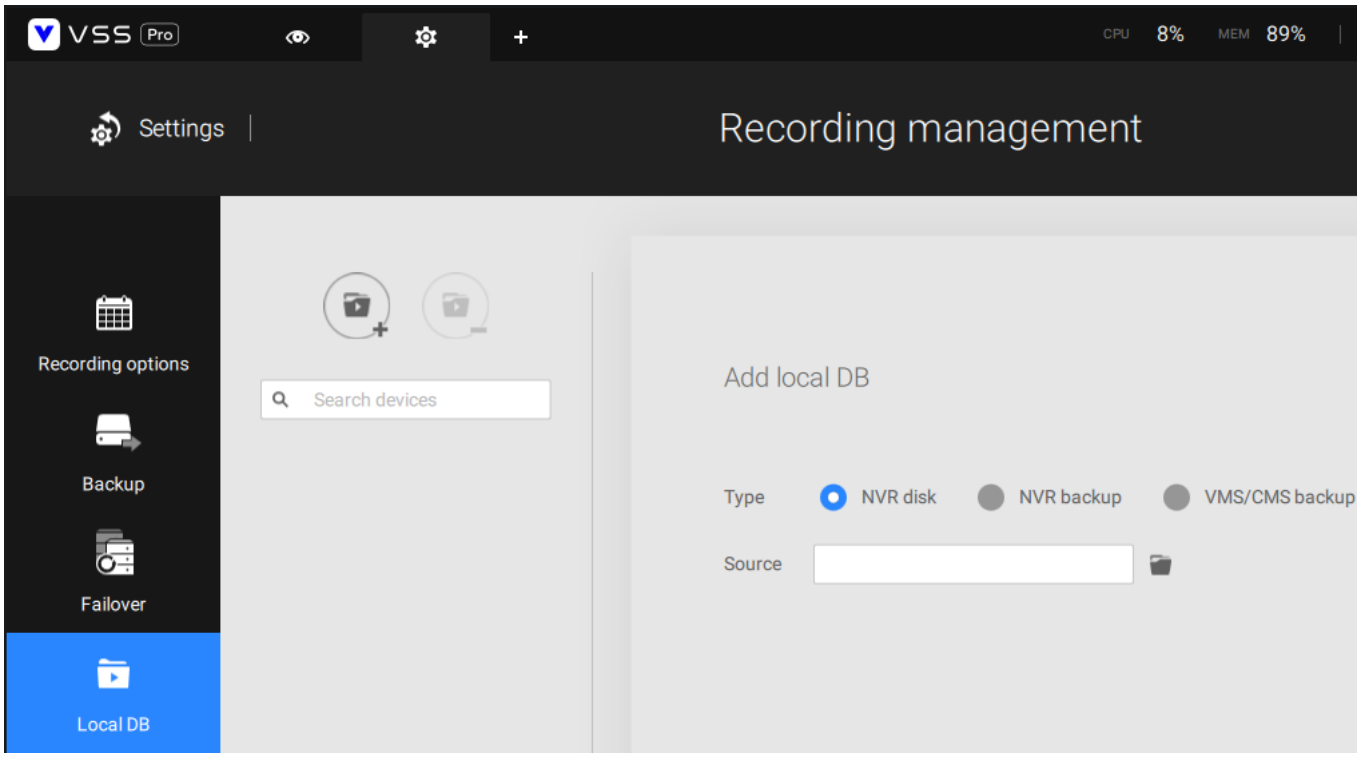


3. From VSS, enter **Settings** > **Device** > **Local DB**.
4. There are 3 import types:
    1. **NVR disk**: the drive tray box removed from a mobile NVR.
    2. **NVR backup**: the recorded videos exported from an NVR using a USB thumb disk or portable drive.
    3. **VMS/CMS backup**: scheduled backup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

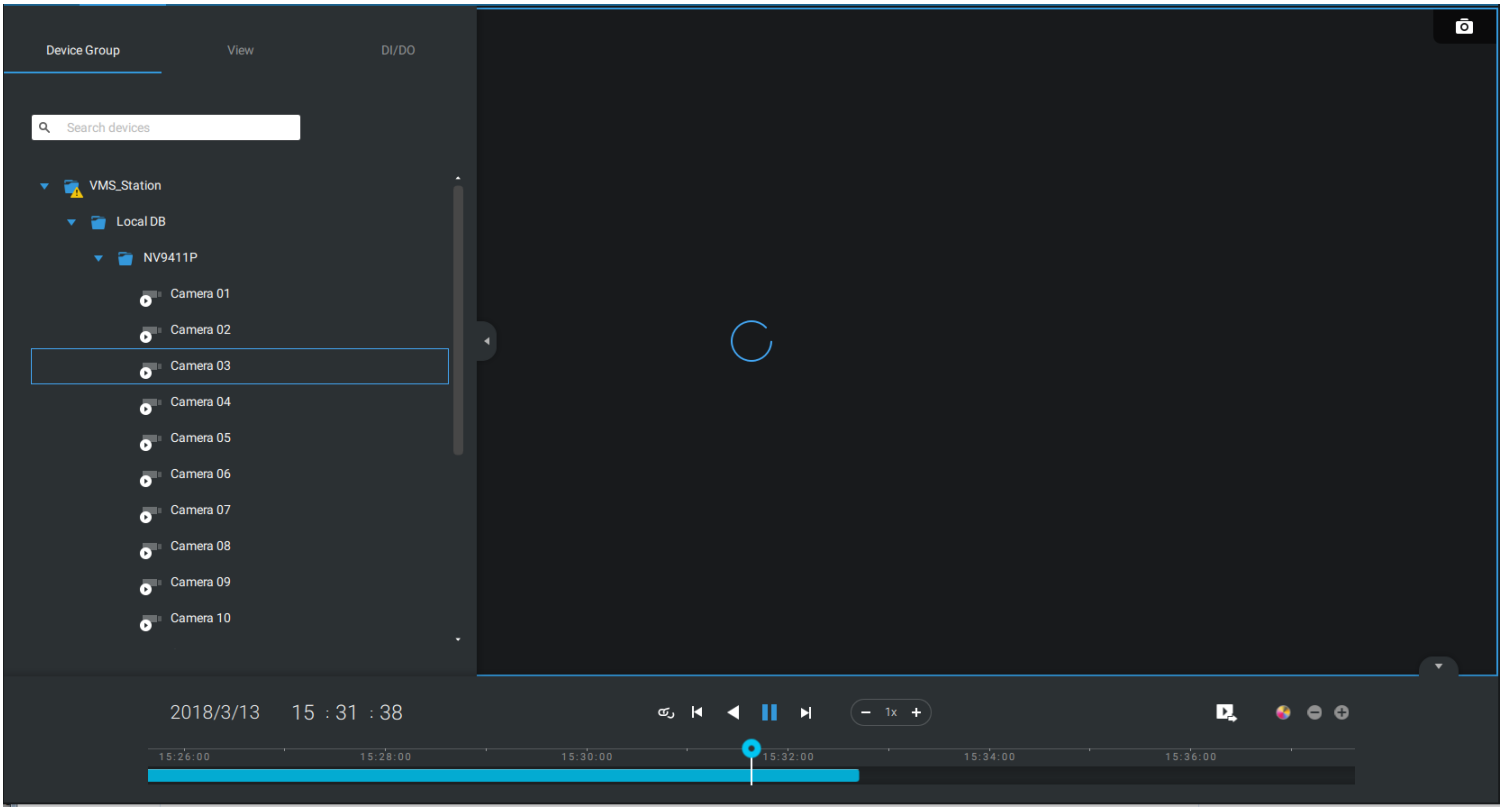


5. Taking a mobile NVR's disk drive as an example, click the Source select button to locate the disk drive.

6. The NVR will be mounted as a local DB.



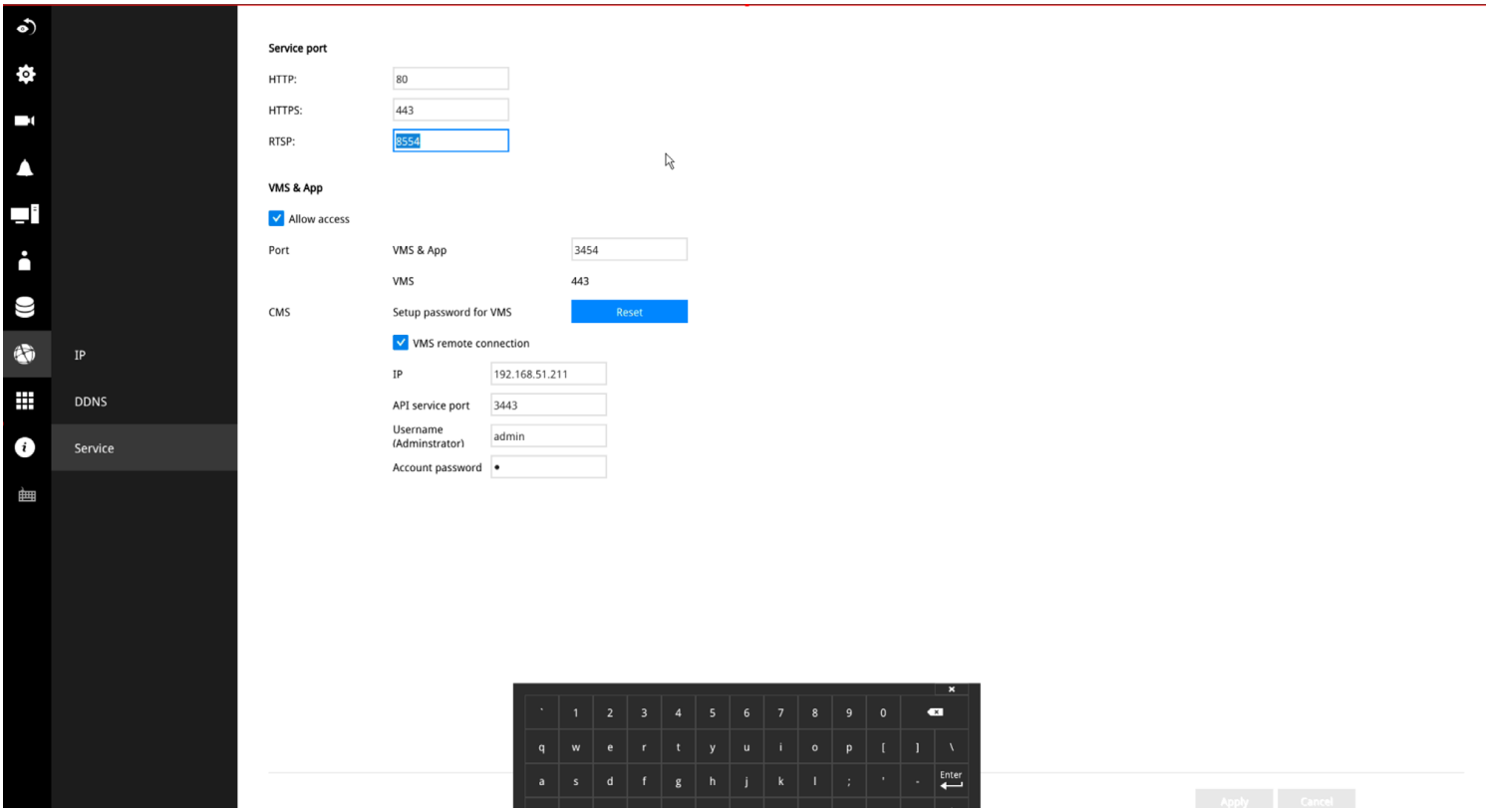
7. A Local DB sub-tree will be listed under your server, and you can view the existing recordings on the NVR's disk drive.



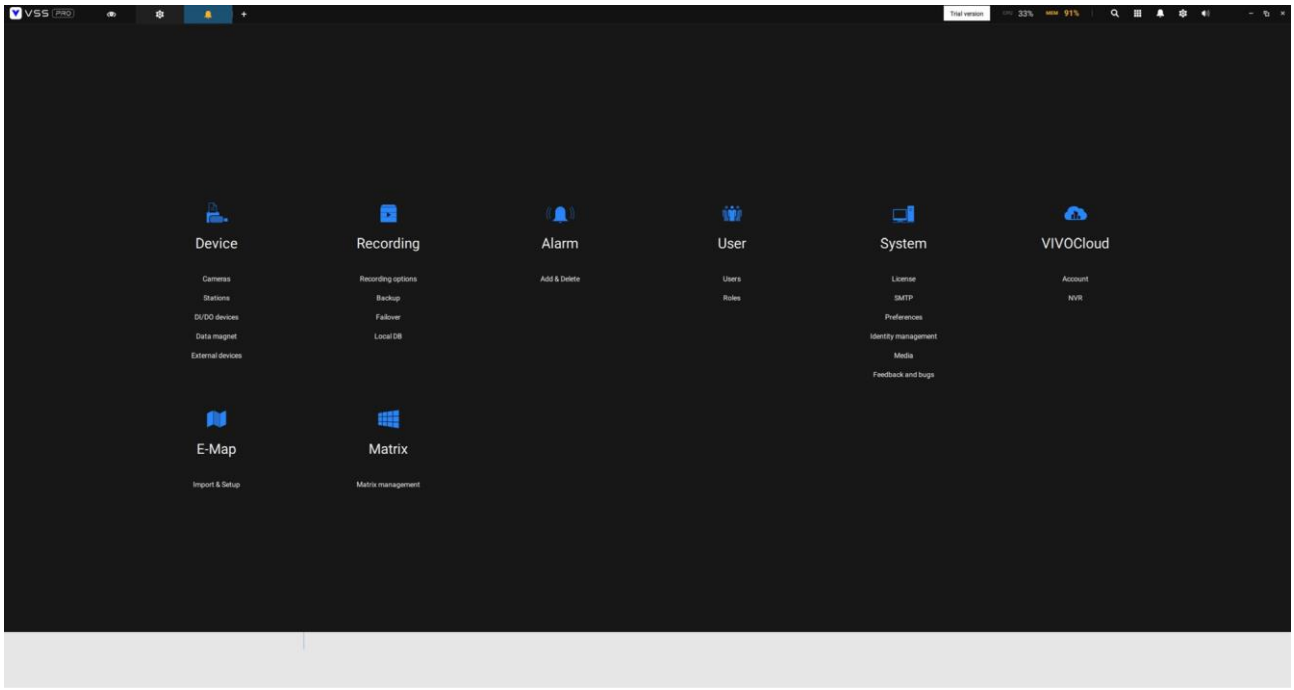
4-9. Settings > VIVOCloud

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

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

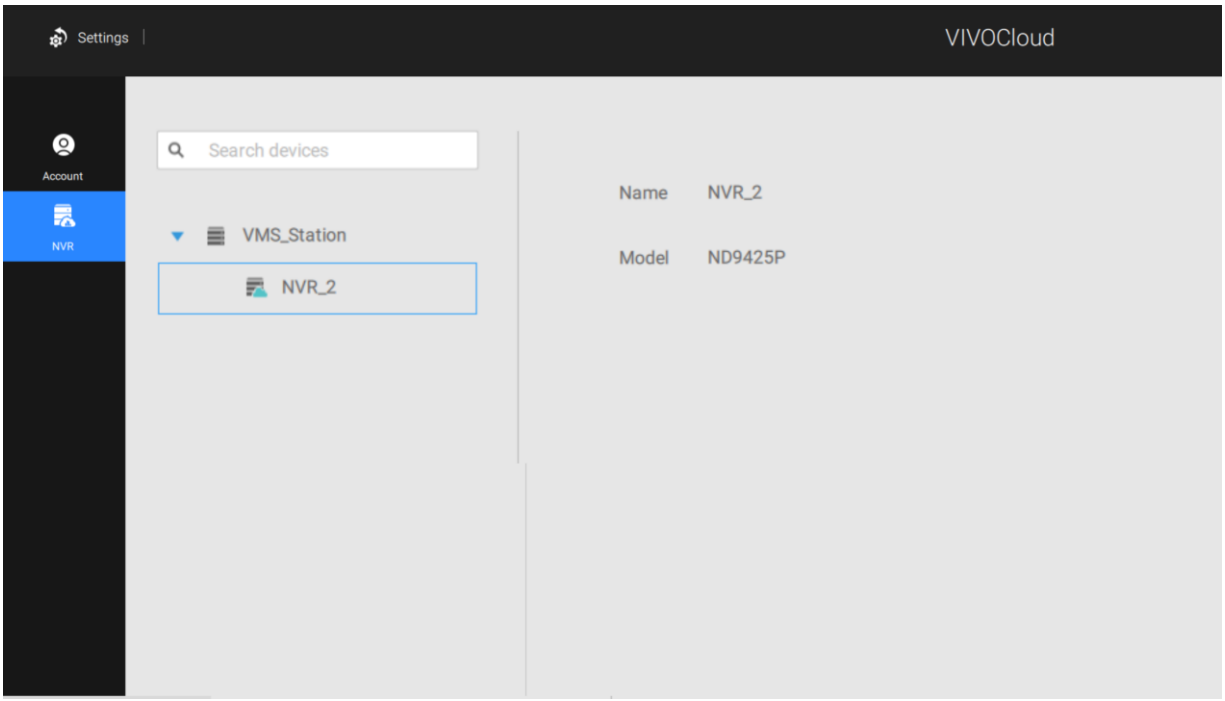


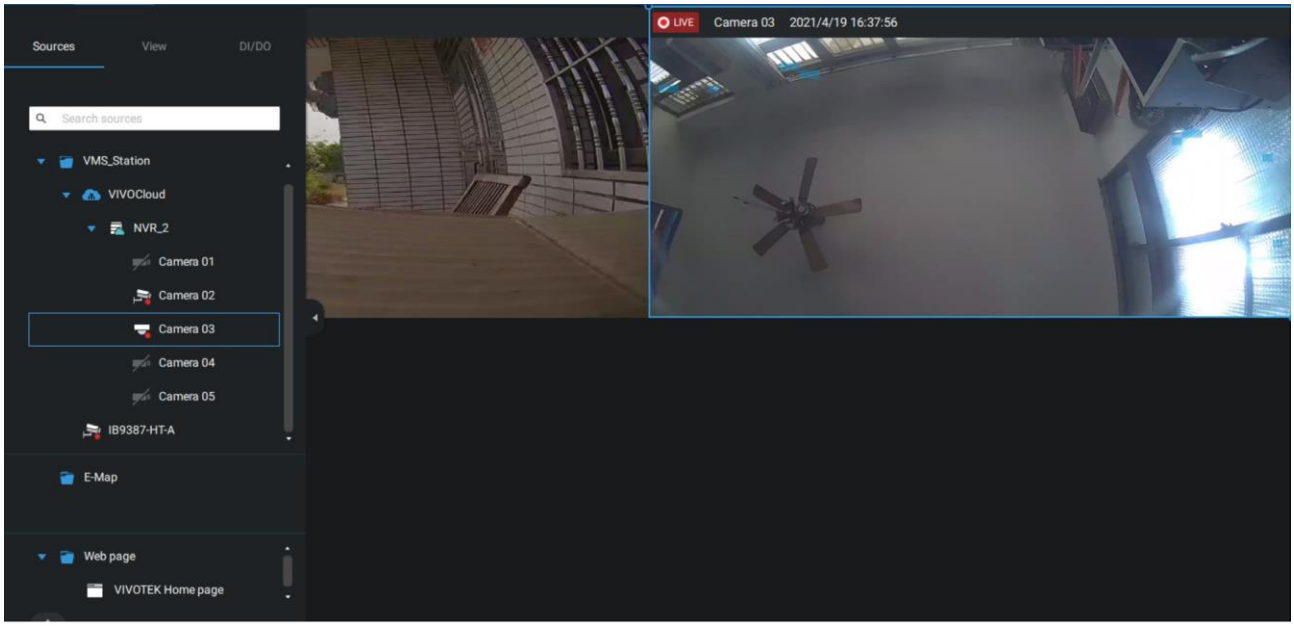
On the VSS client, click Settings > VIVOCloud



Log in using your VIVOCloud credentials.

The NVR will be listed under the VIVOCloud device tree.



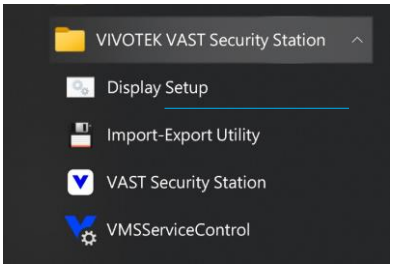


If the NVR managed through the VIVOCloud is connected via a local or P2P network, the connection should be normal. If the NVR is connected through VIVOCloud Relay, a 28 minute timeout will be imposed, and you can use the connect button to re-connect.

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

Appendix A: VSS Service Control Tool

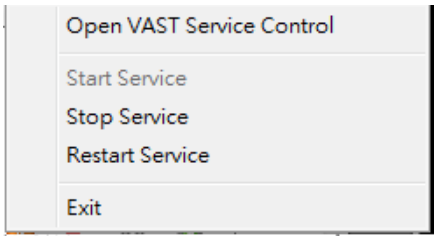
VSS service control tool is a tool for server control and for user to be aware of the VSS Server status. It starts up as Windows OS startup.
Under Microsoft Windows, choose "**Start > All Programs > VIVOTEK Security Station > VMServiceControl.**"

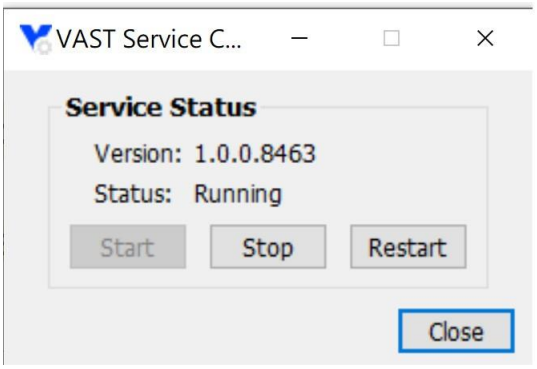


You may also find it in the system tray icon of the tool bar, which indicates that the service is running: 

It shows a disconnection icon when the service is stopped: 

A menu for the service control tool will pop up when you **right-click** on the icon:

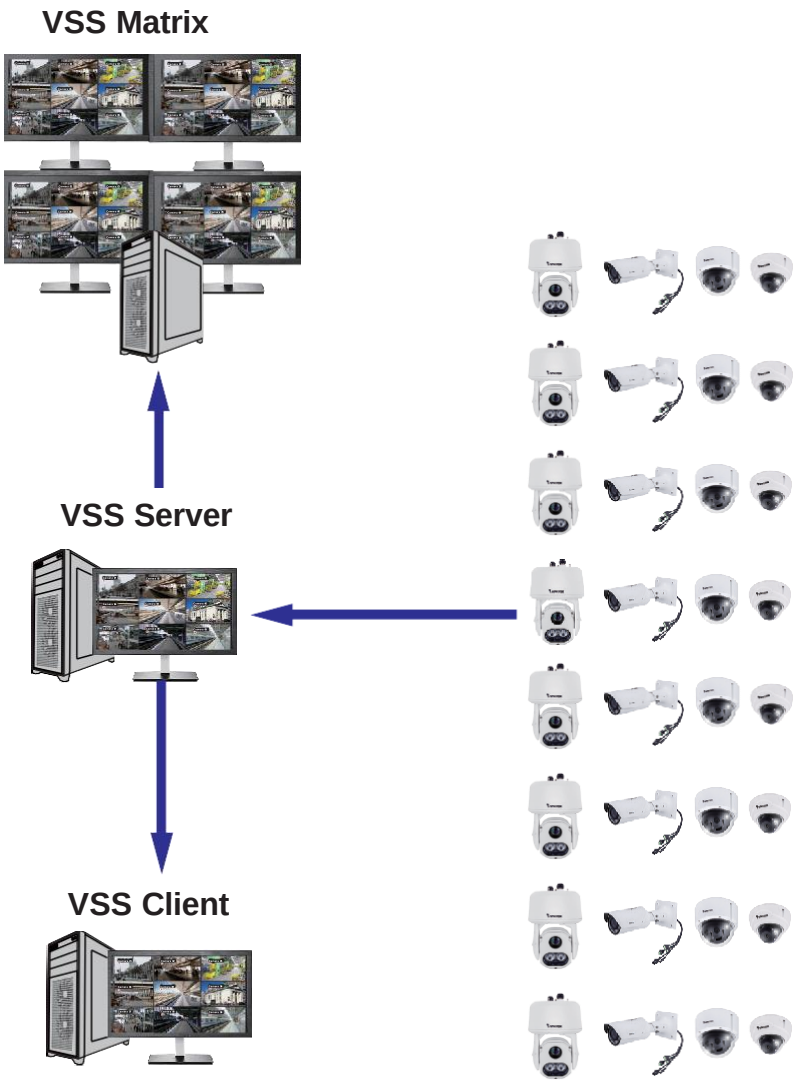




Here you can manually start, stop and restart the service.

Appendix B: Matrix

The virtual matrix feature enables the display of any cameras on any monitors in an IP surveillance network. Combinations of live or playback streams can be displayed simultaneously. In addition to pre-configured live views, E-maps, Google maps, and Alarm panes can all be placed on a remote matrix. Users gain real-time awareness of scenes and access to past events.

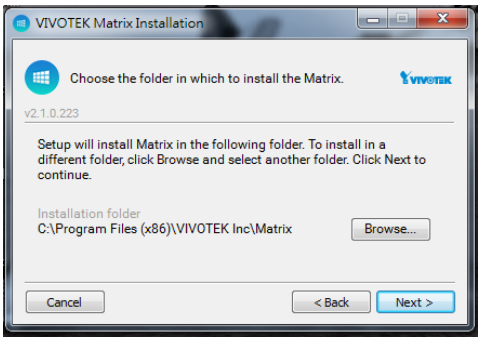


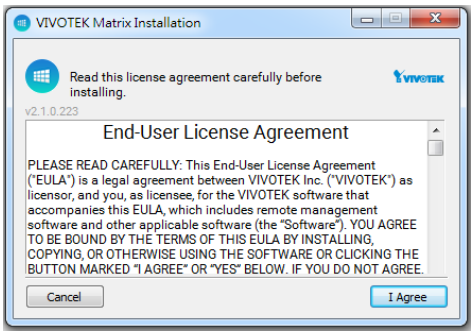
Prerequisites:

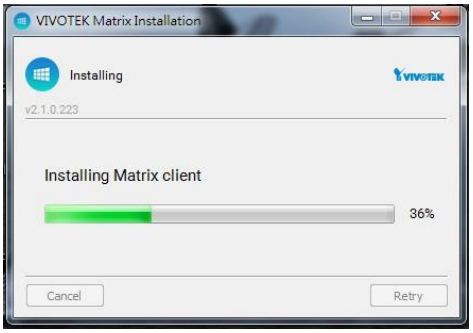
1. One VSS server and another computer running the Matrix client utility.
2. The first 2 digits of software revision numbers of VSS server and Matrix client must be the same: e.g., 2.3.x.x and 2.3.x.x.
3. Sufficient network bandwidth among network cameras, VSS servers, and Matrix clients.

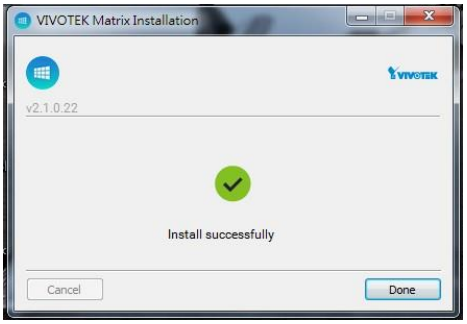
Configuration procedure:

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

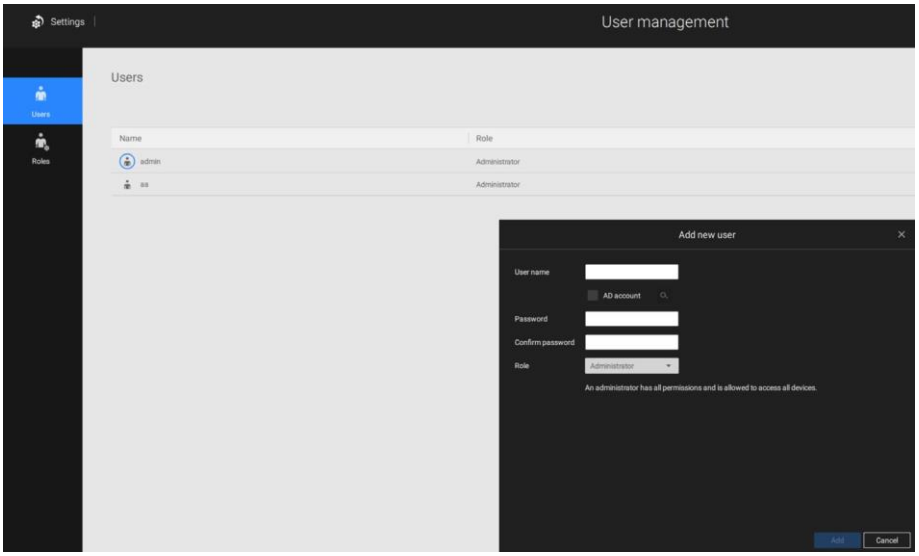




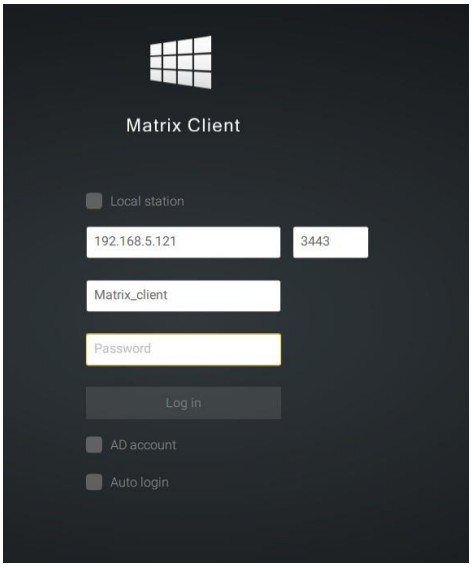




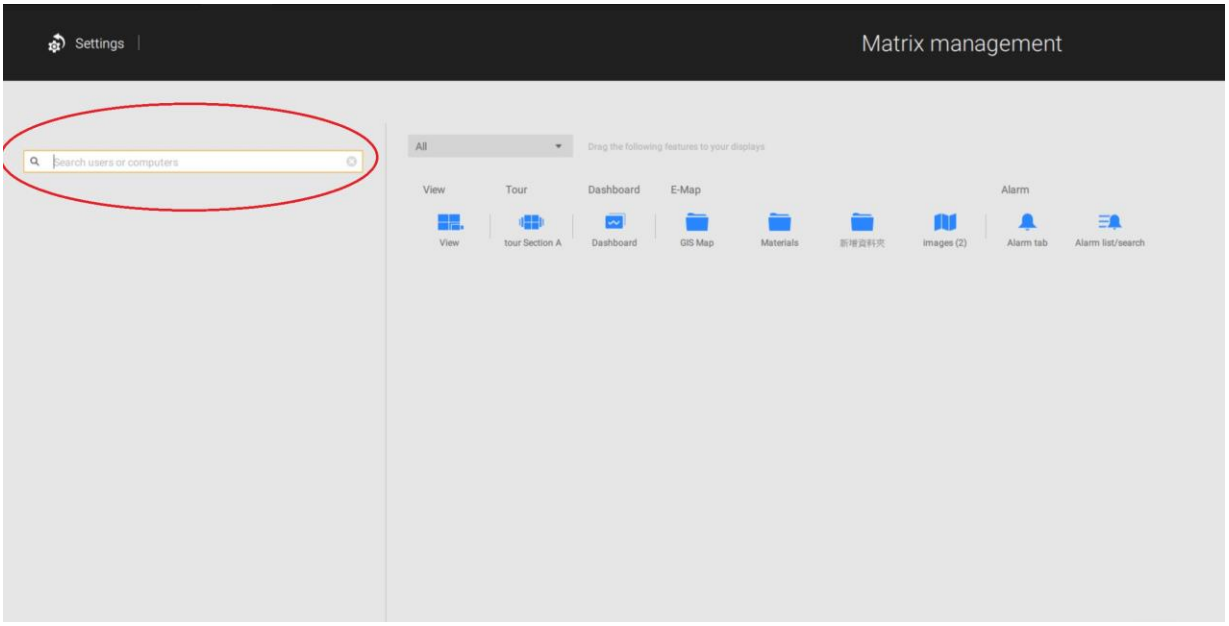
2. On the VSS server, create a user account for the Matrix client. Depending on the operation on the client computer, assign the client user with adequate operation privileges.



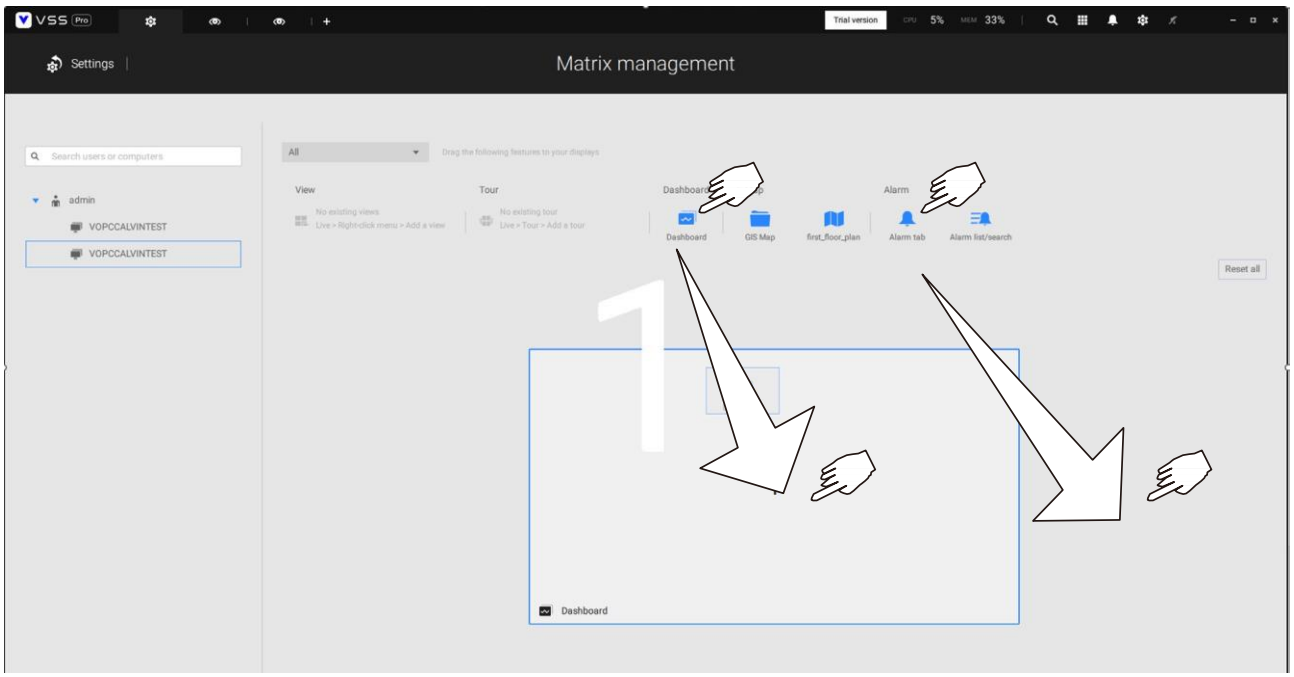
3. Open the Matrix utility, log in to the VSS server address, using the Matrix client account credentials.



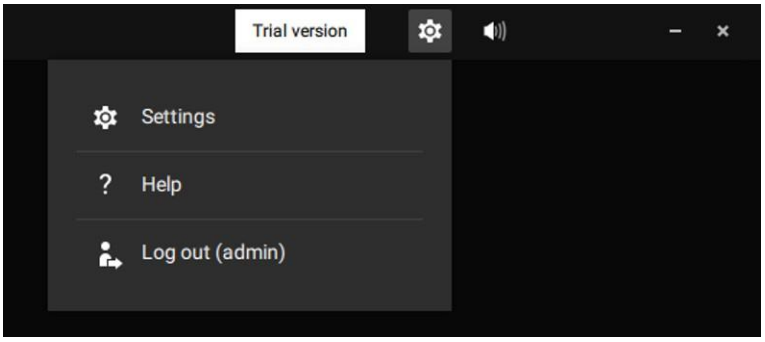
4. From the VSS server, open the Settings > Matrix Management window.
5. Enter the name of your Matrix client, e.g., Matrix client in the search panel of the Matrix Management window. Note that the Matrix client must have logged in to establish the connection before the VSS server can find it (as previously described).



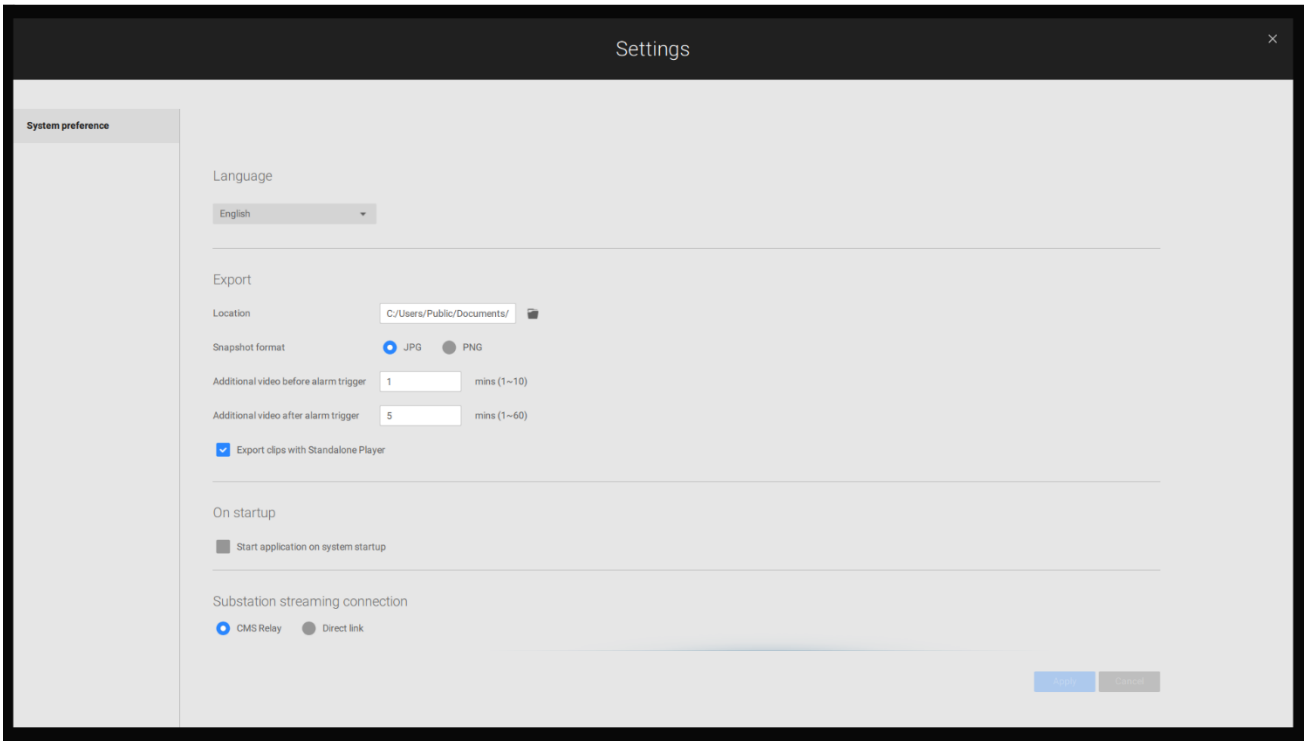
6. Once the VSS server finds the Matrix client, the available monitors will be listed. Click and drag the pre-configured Views, Tour, Dashboard, E-maps, or Alarm panel to any of the monitors.



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.



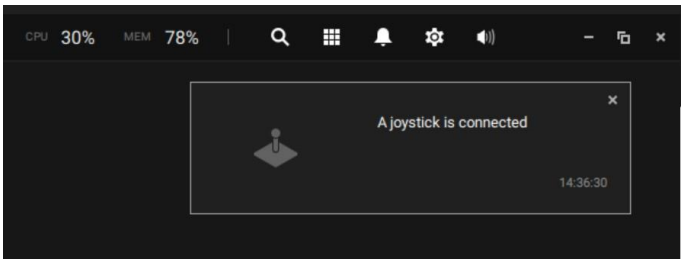
If necessary, change your client settings. Here you can change the displayed language, Export target folder, Start-up option, and the streaming connection options.



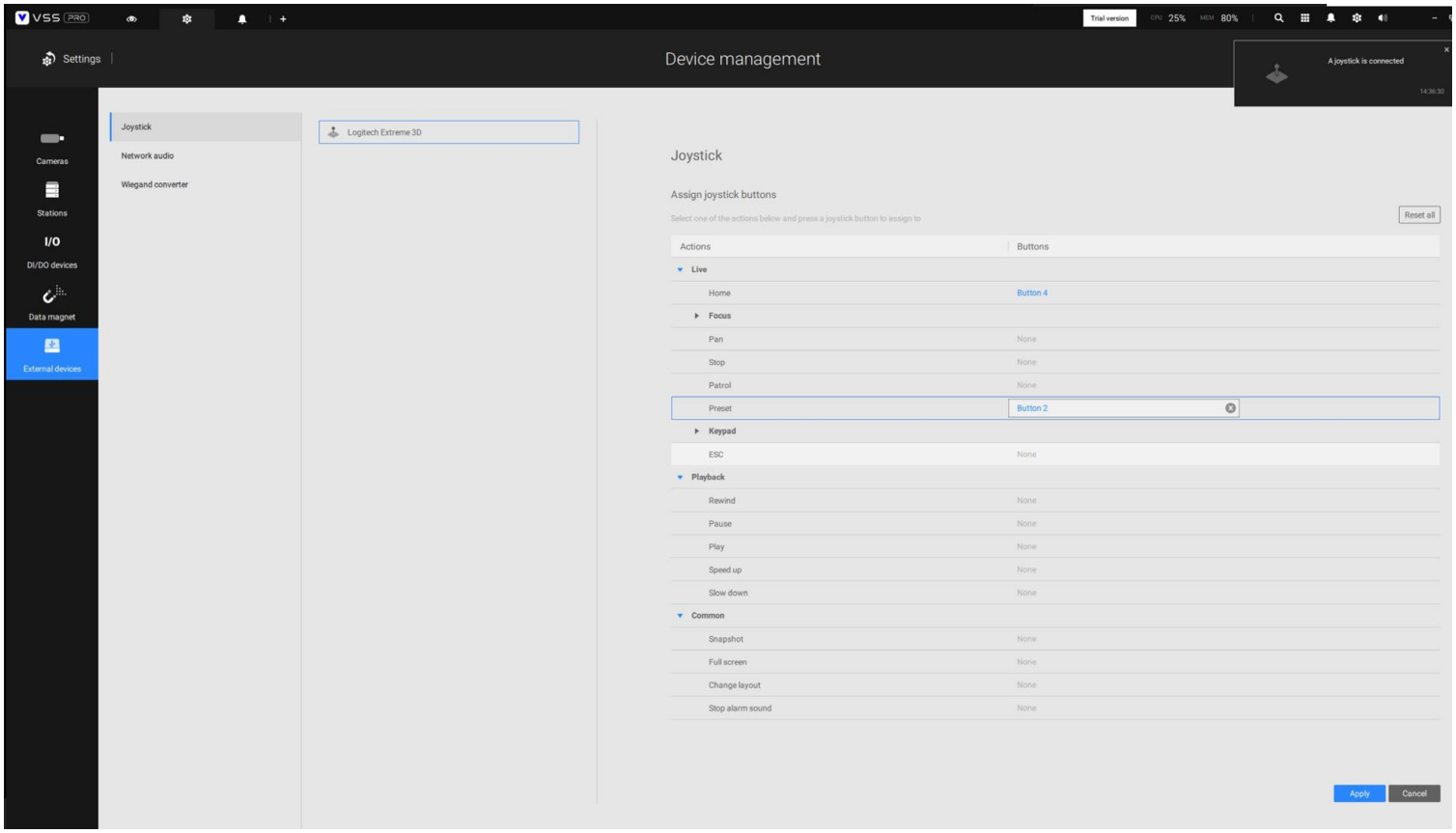
Appendix C: Joystick Support

Configurable joystick buttons

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



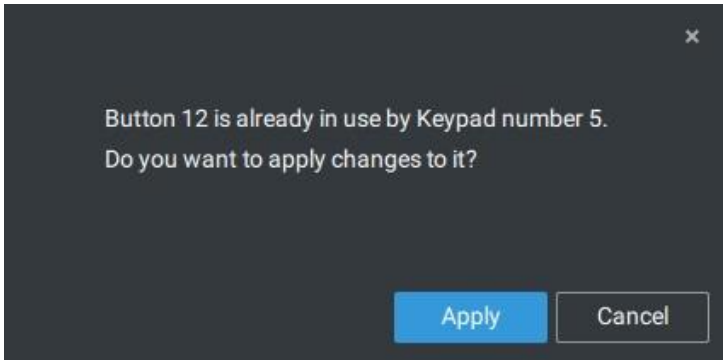
3. Enter **Settings** > **Device** > **External devices**.
4. Single-click to select the detected joystick. The configurable buttons will be listed. Click ▶ to expand the **Live**, **Playback,** and **Common** menus.



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

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

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



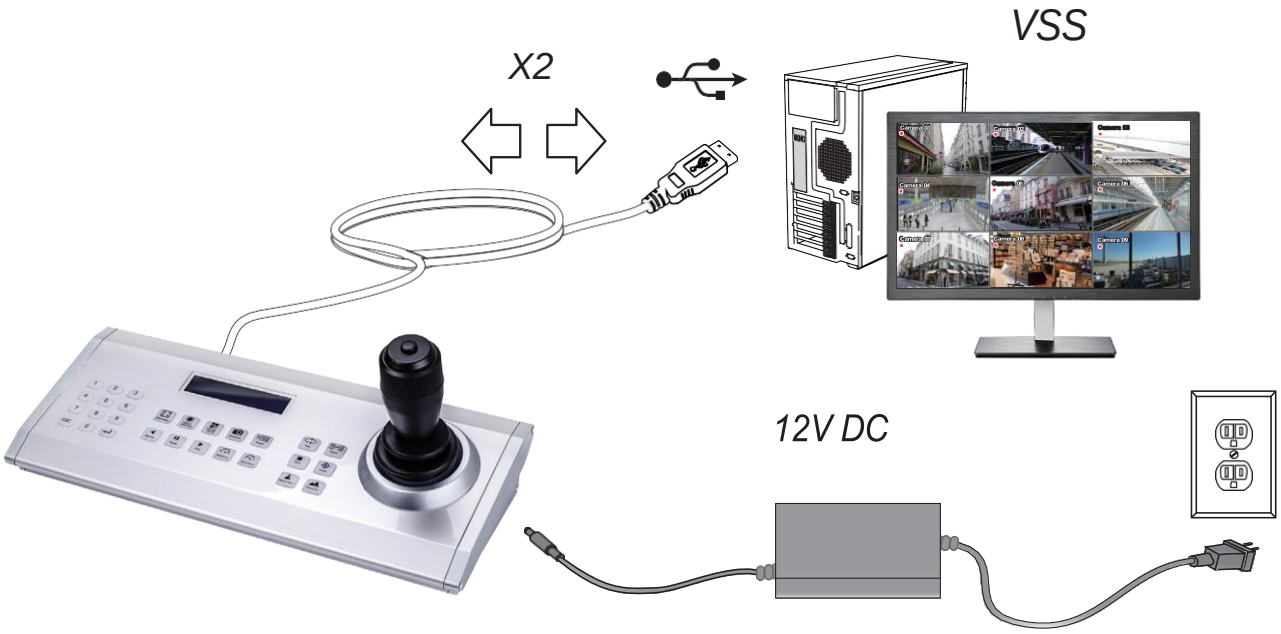
Repeat the above process and click the **Apply** button to preserve your settings.

VIVOTEK's joysticks

The AJ-002 is a USB joystick with HID 3-axis PTZ control, a twist wheel for zoom in/zoom out, and 29 configurable function buttons for use on a VSS 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 VSS server.

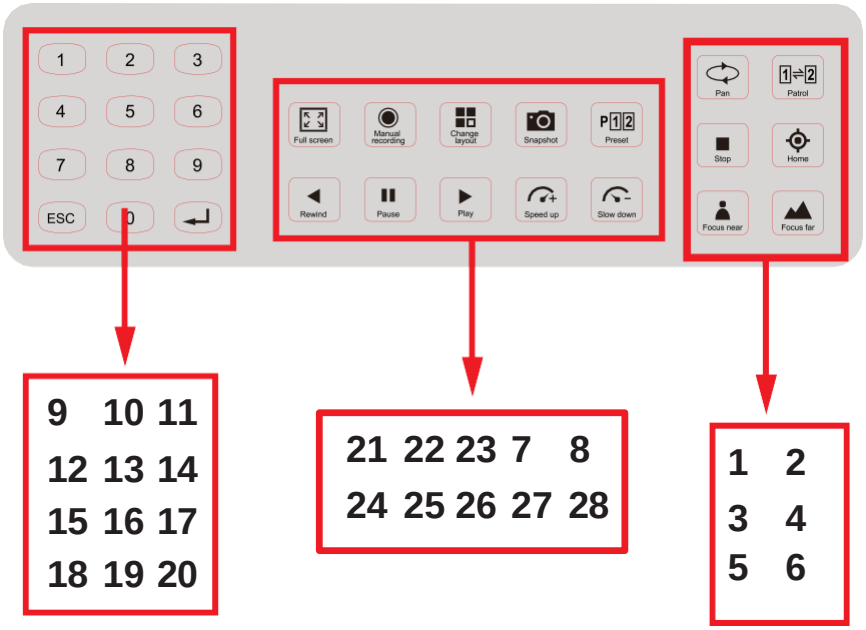


NOTE:

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

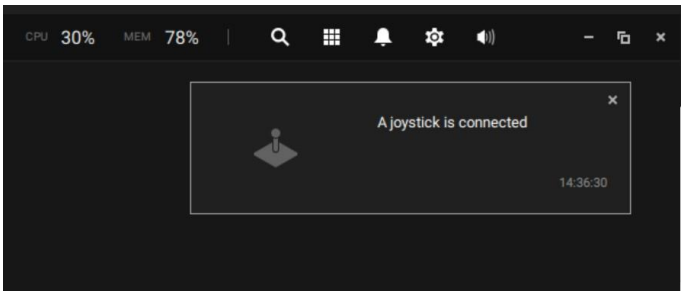
Below is the keypad numbering sequence:



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 VSS server should automatically detect the connection.

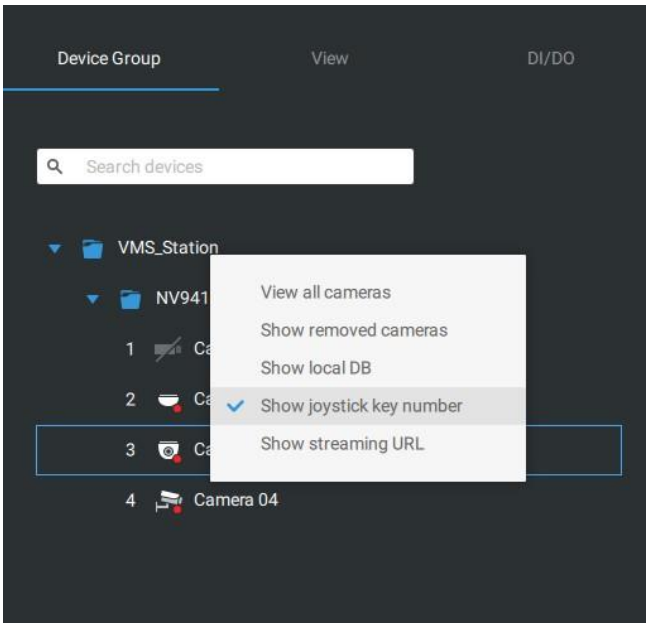


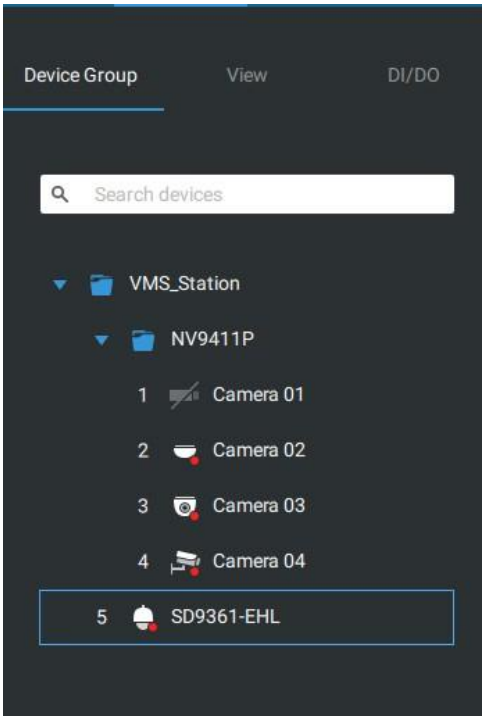
The following controls are available:

* PTZ control – Basic PTZ control: Direction, Home, Zoom in/out, and Focus near/far.
* Playback control – Play, Pause, Stop, Rewind, Speed up and Slow down.
* View switch – Switch to existing View (Users need to create views first).

Left-click to select your server on the device tree, and right-click to display and select the "**Show joystick key number.**" The camera key numbers are determined by the sequence when the cameras were added to the VSS configuration, and cannot be changed. By default, the key numbers are not shown.

Press the key number on the joystick keypad and the Enter key ↵, e.g., 5 + ↵. The full view of the selected camera will display.





Press the ESC key to leave the full view.

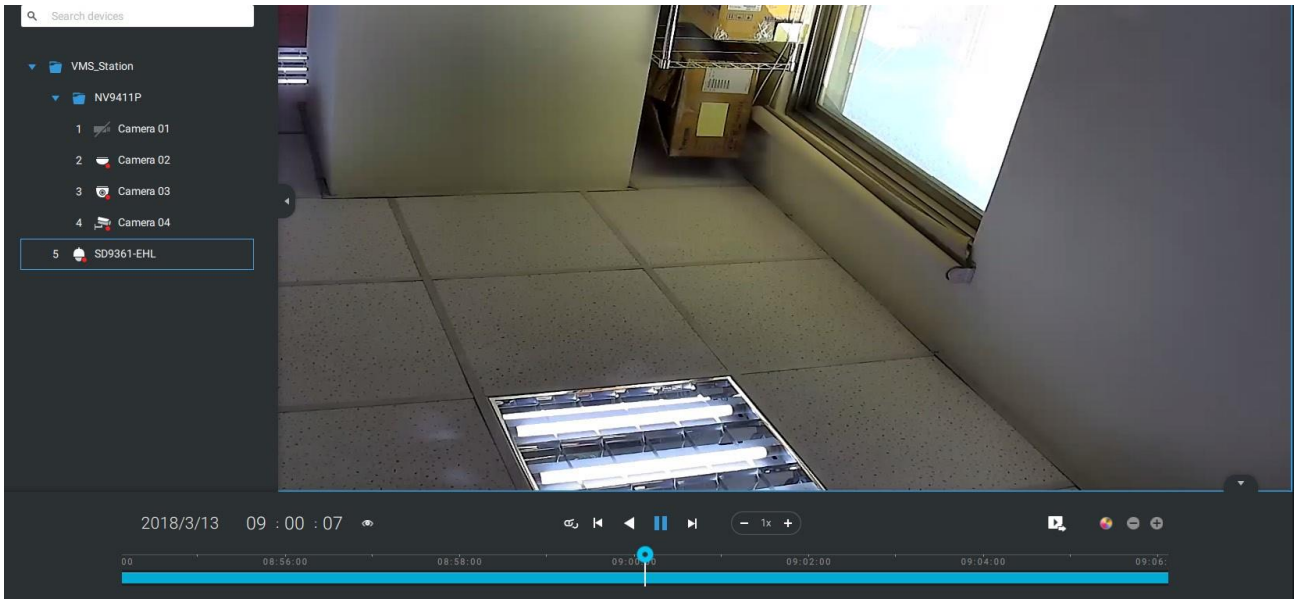
To move to a preset position, press the number key + Preset, and the Enter key ↵. The number key corresponds to the sequence number for the preset position regardless of the name of the preset.

Note that the RS232/485 terminal connection is currently not supported.

Note that the Manual Recording button is currently not effective.

If you have multiple views, press the number key and the Change Layout, and the Enter key ↵ to switch to a different view. The number key corresponds to the sequence number for the view you configured regardless of the name of the view (layout).

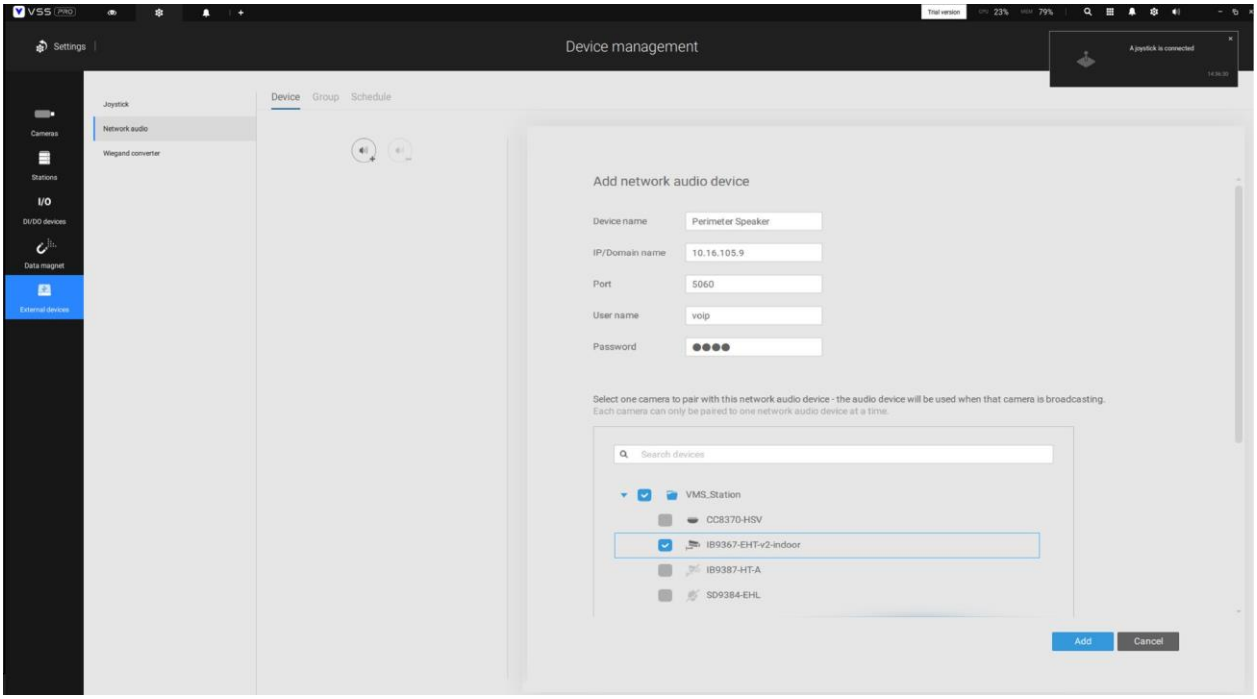
The Play button toggles the playback window. From here you can trace back the past recordings. You can use speed up, slow down, and rewind buttons here. Once the Playback mode is toggled, the point-in-time defaults to the start of the current hour.



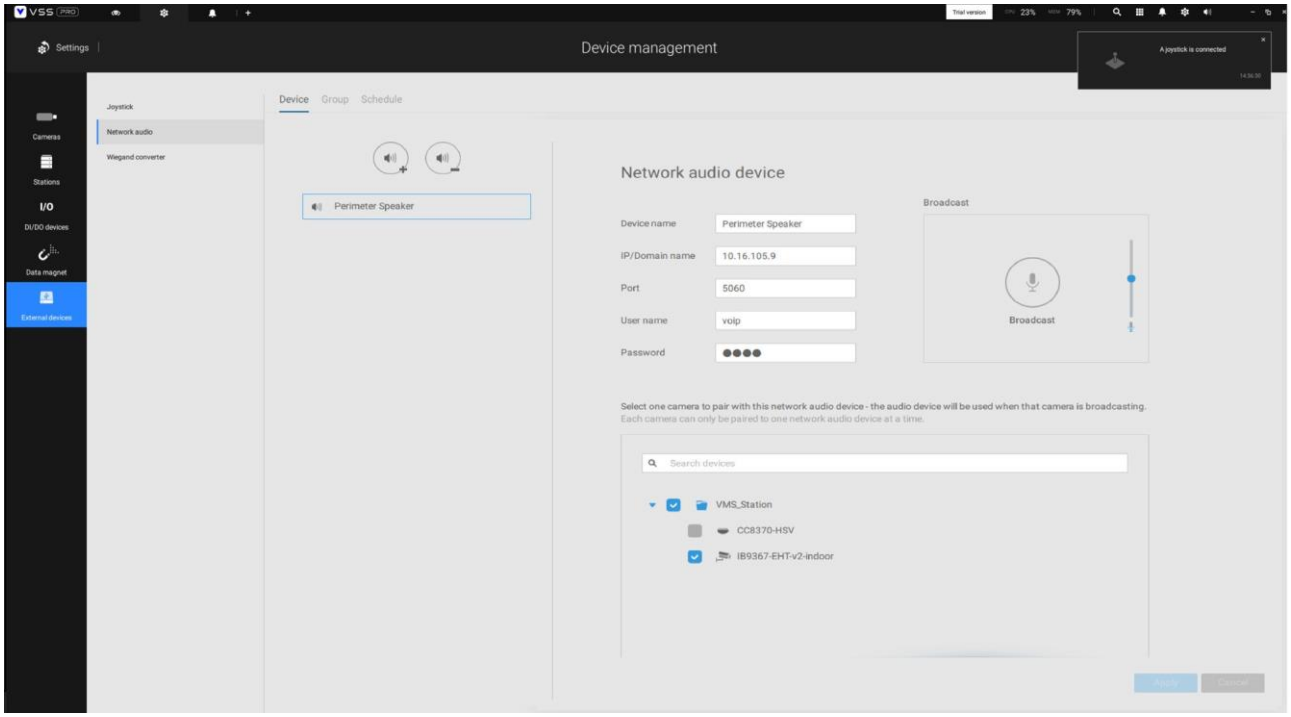
Appendix D: Network Audio Solution

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.

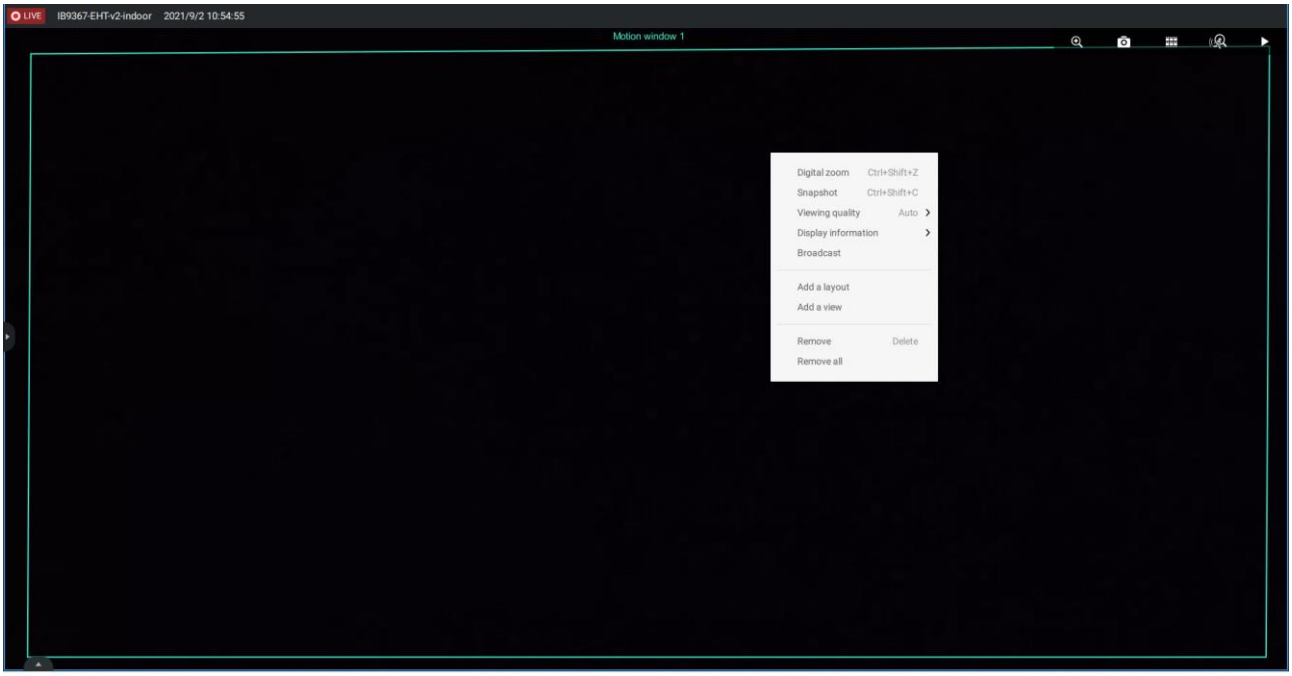


4. You can use the Broadcast function on the right of the screen to test the connectivity.
5. You can right-click on the live view to find the Broadcast function to speak or broadcast an audio clip.

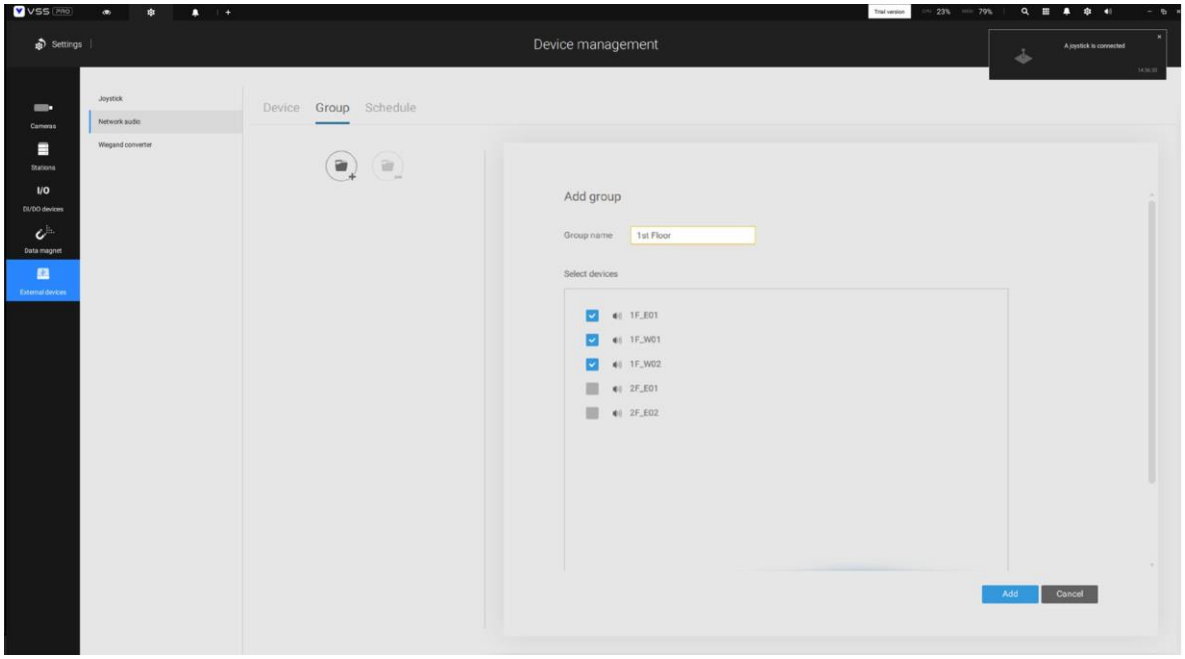


6. On the occurrence of a triggered alarm (Motion or VCA event), you can configure the alarm settings so that the system can broadcast an audio clip. Configure audio clip settings in System > Media, and select "Play audio file with network audio device" in the Alarm action page.

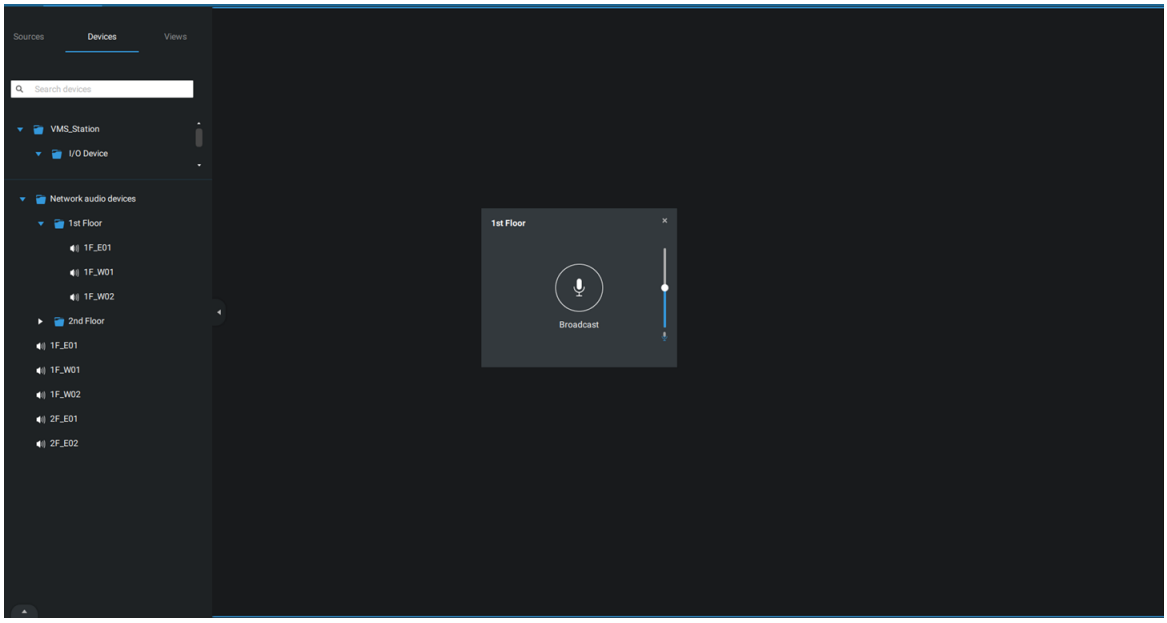
Note that the pre-recorded audio clip should be uploaded from System > Media. The supported audio file is WAV: 8Khz, Mono, 16-bit, PCM.



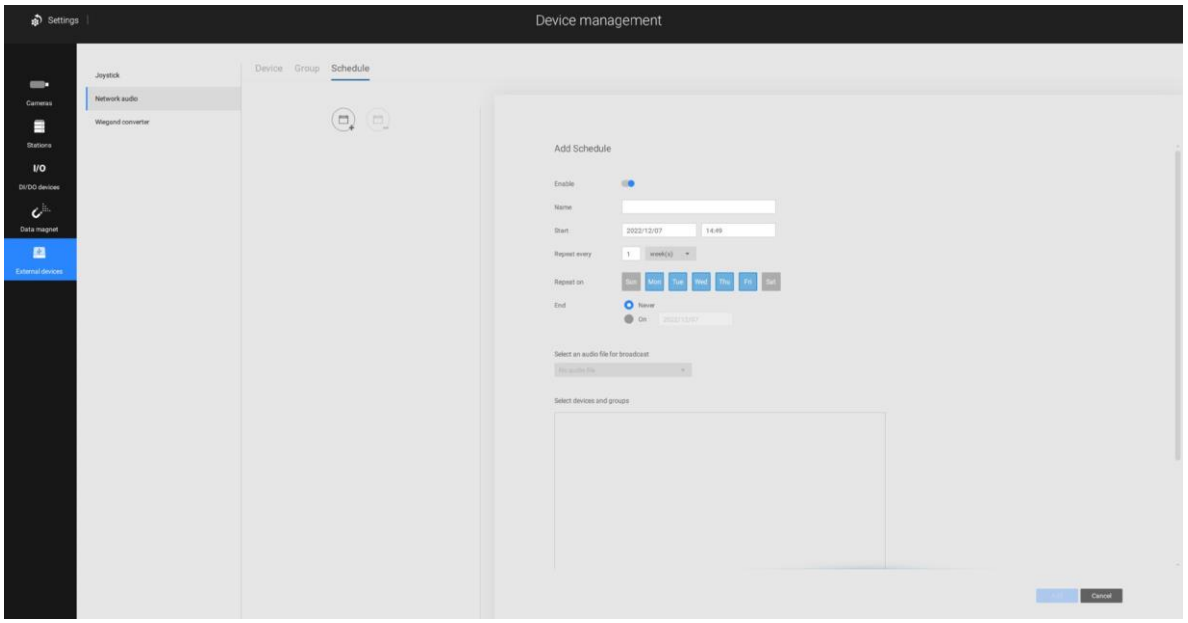
You can create groups for different audio devices. Use the Group tab to create audio groups. Select devices for the group.

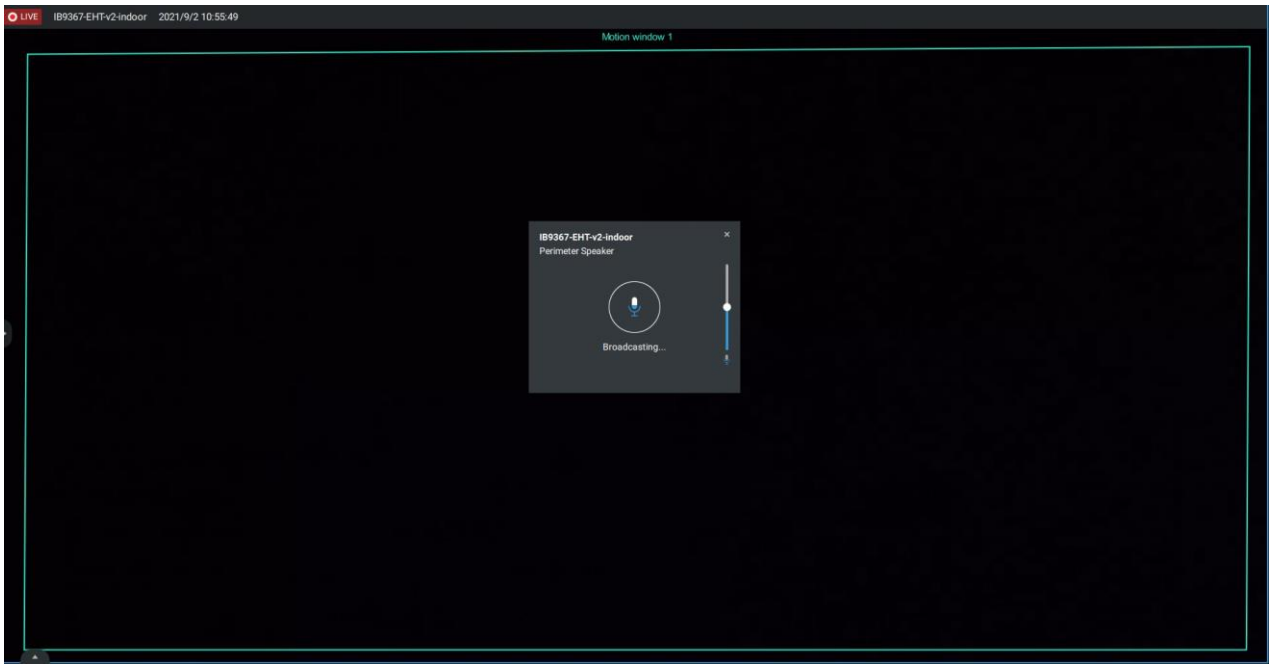


With audio groups, you can select audio devices from the Devices tab on a live view so that you can broadcast audios to a group of devices.



You can create a schedule to play a pre-selected audio file. In Network audio > 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.

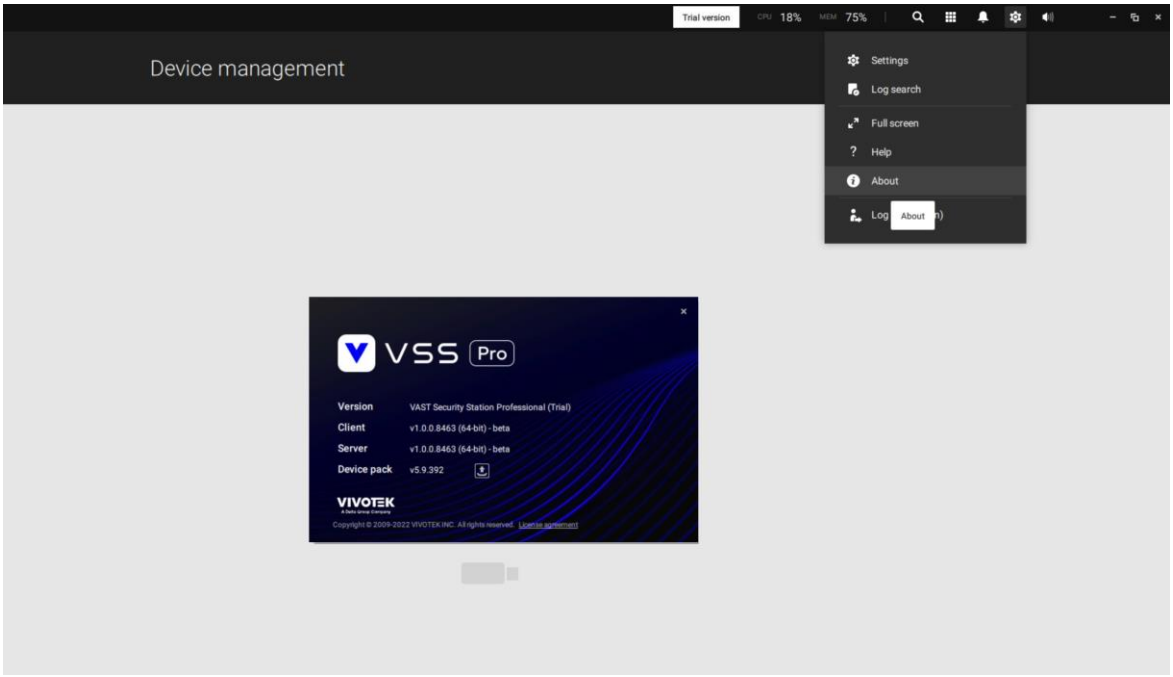




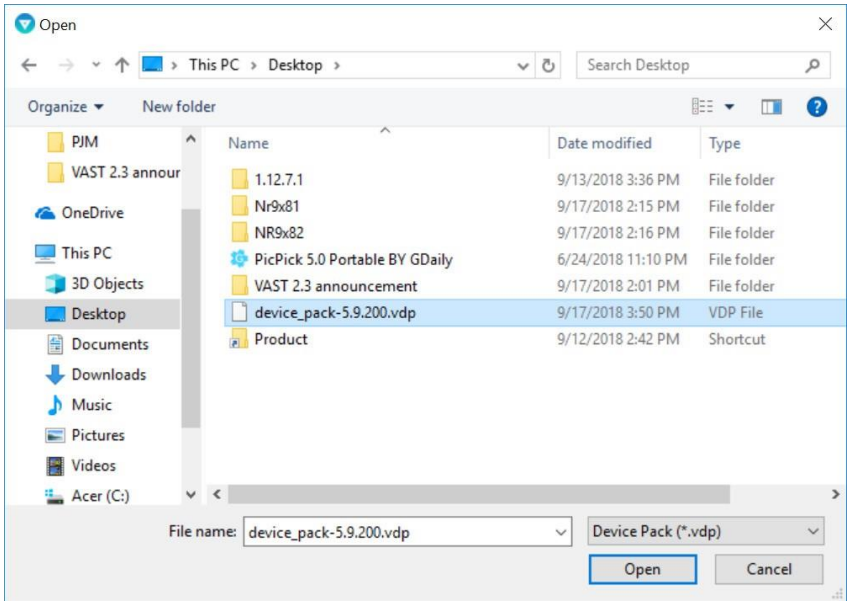
Appendix E: Upload Device Pack

A device pack is constantly 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 VSS server. New functional parameters and functions in the new cameras are available through the device pack.

Enter Settings > About to see the upload button.



A device pack file looks like the following.

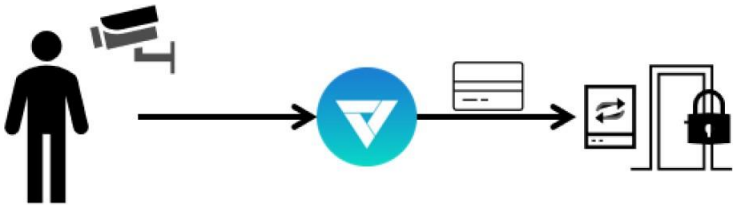


Appendix F: Multi-factor Authentication for Access Control

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 recognitions succeed, the gate will open allowing the driver to leave.

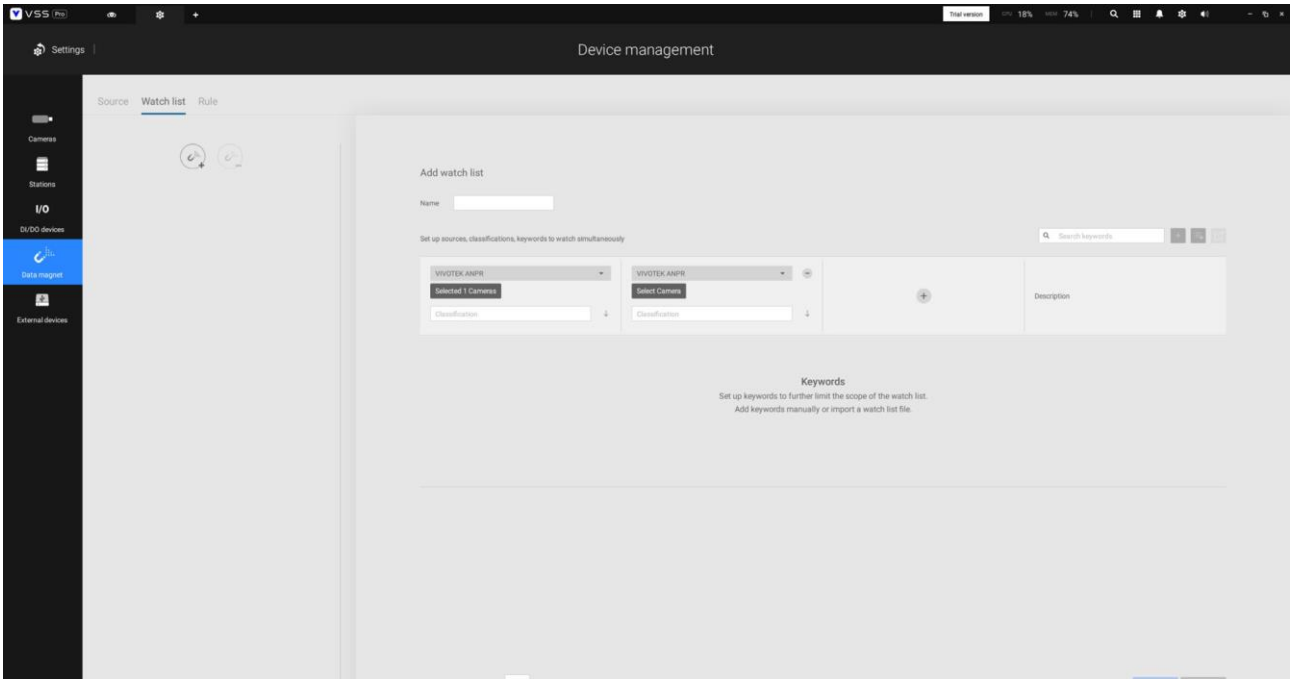
In an office, an access control system can be combined with Face recognition mechanism to avoid someone using someone else' card to cheat the attendance system.



The scenario shows one holds an ID card and via the Face recognition system, his identity is verified as one employee in the database. VSS 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.

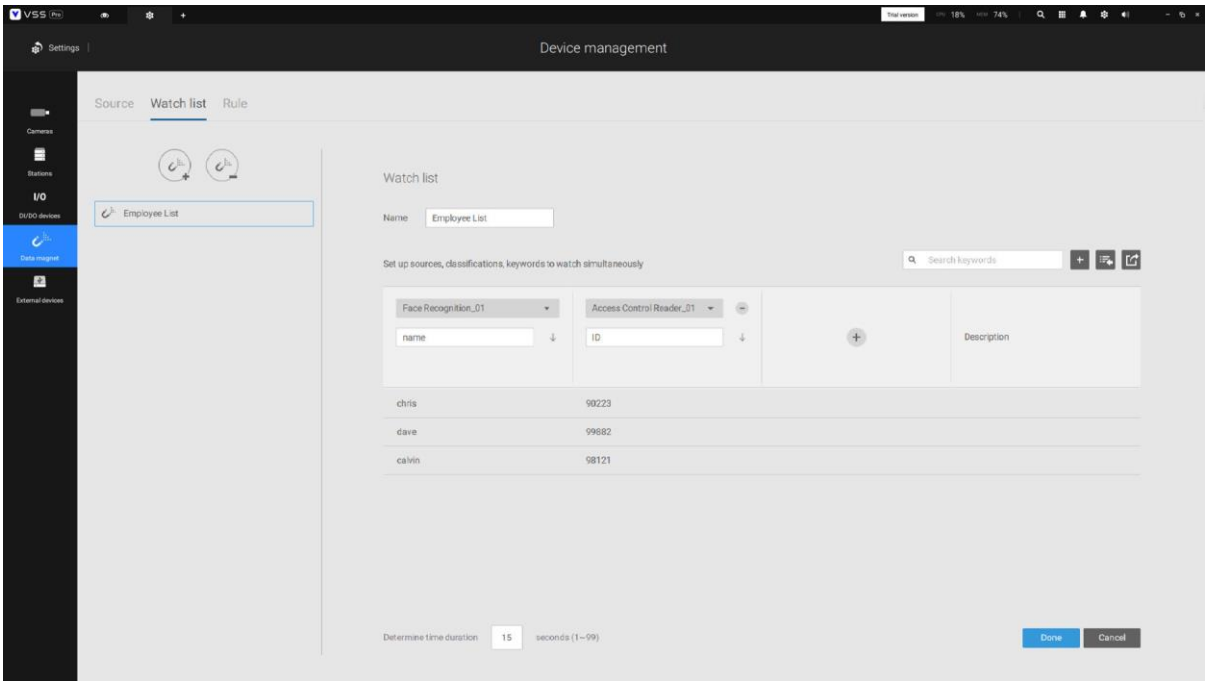
To acquire data from multi-factor systems, we use the Watch list on Data Magnet.

1. Depending on your applications, configure multiple data magnet sources, so that data can be transferred and acquired by VSS.
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.



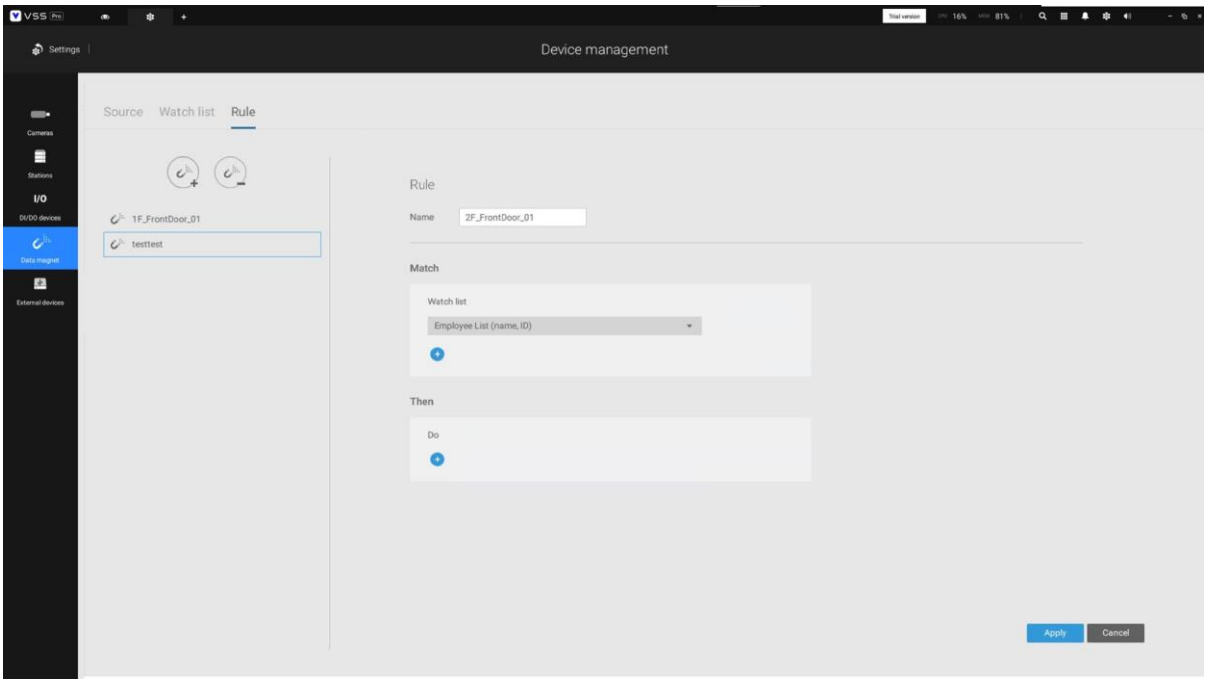
3. Click the Add item button and enter a name and employee ID such as one for an employee. Click Add to finish, and repeat the process for more items.

4. At the lower screen, enter the time threshold for receiving data from multiple sources. For example, If set to 15 seconds, VSS 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?"

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

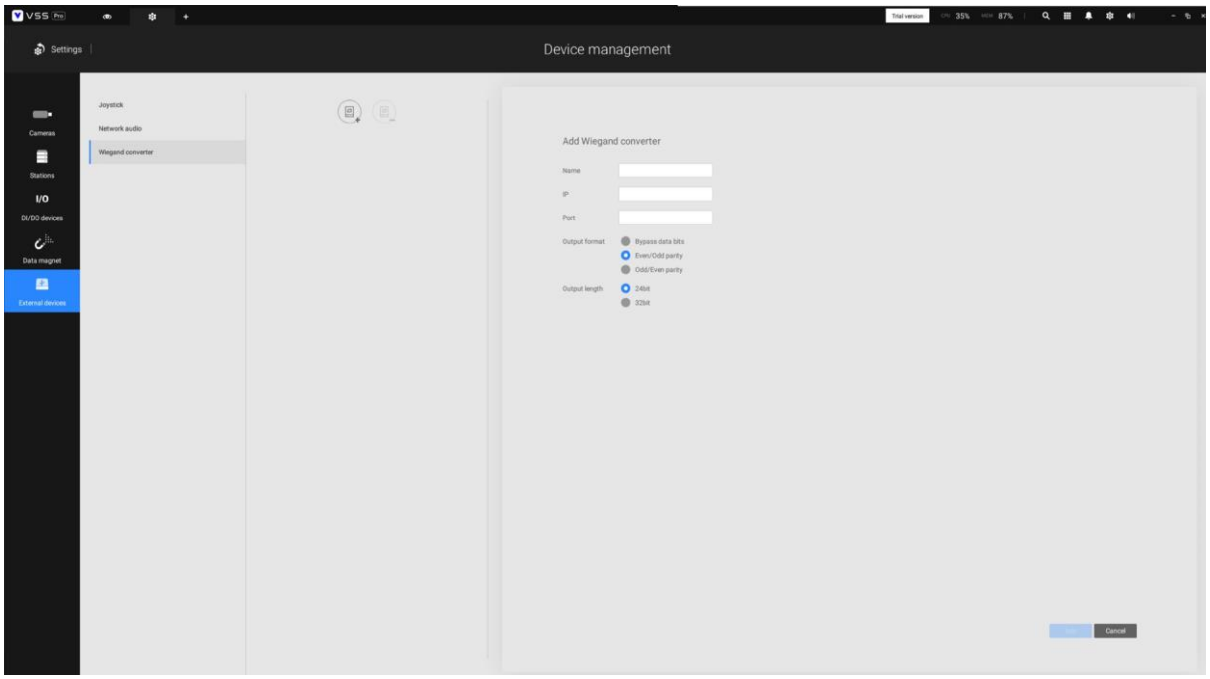
The Wiegand converter can transfer the ID Badge card number through the Wiegand protocol to an access control system. The access control system then decides whether to open a gate or not. The VSS station sends an employee's card number to the Wiegand converter, the Wiegand converter then delivers it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

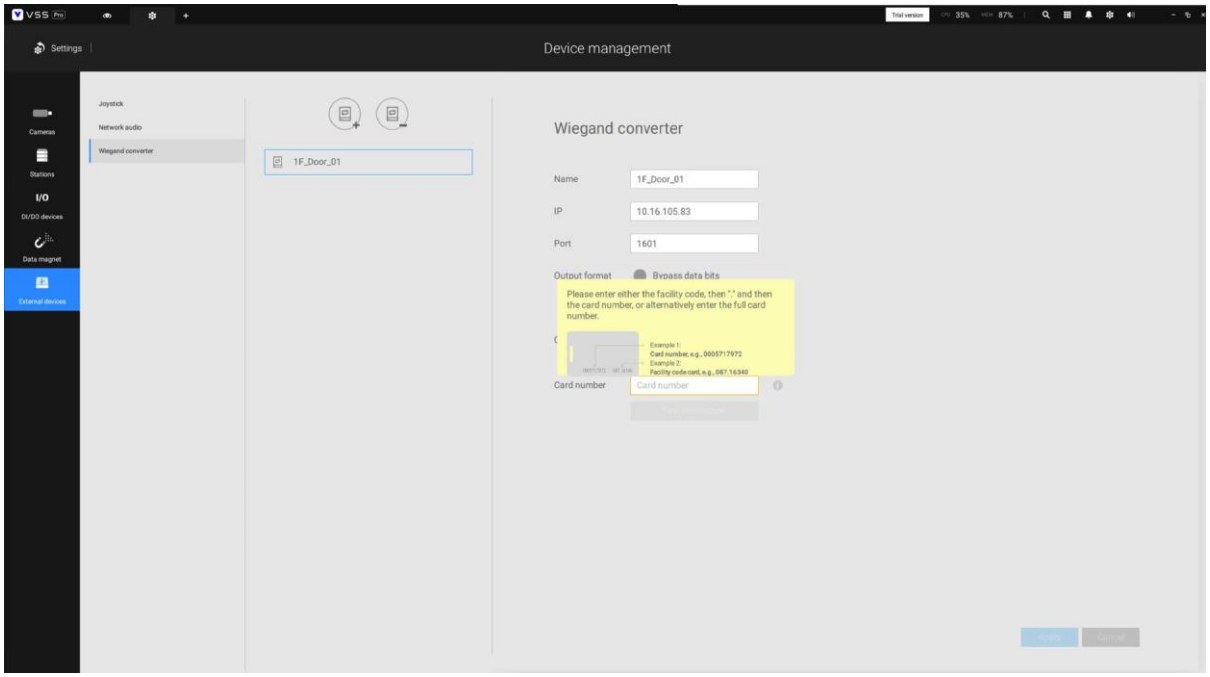
For example, a watch list's employee name=Chris and ID=90223 is verified, you can send the ID card umber to the Wiegand converter. If a watch list's data is not the card number, but the data contains name=Chris, employee ID=90223, you can select "Map data to Wiegand card number." Via the Identity management 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.

How to add a Wiegand converter to VSS?"

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.



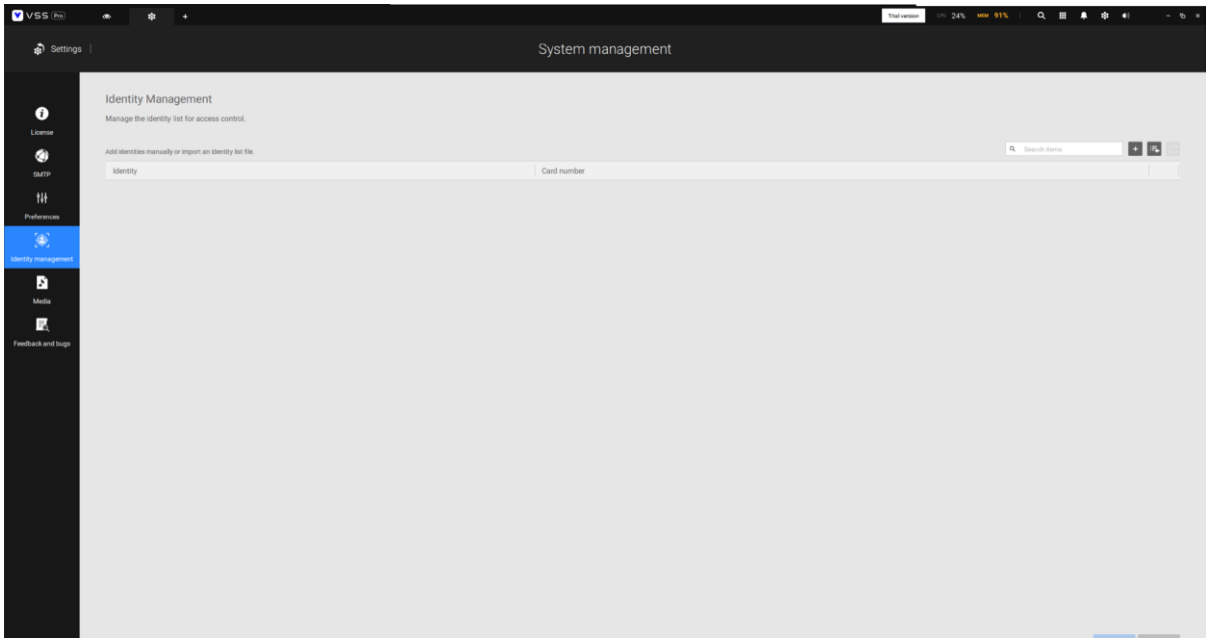
When adding is completed, enter a card number in the Card number field to test if the converter can successfully receive a card number.

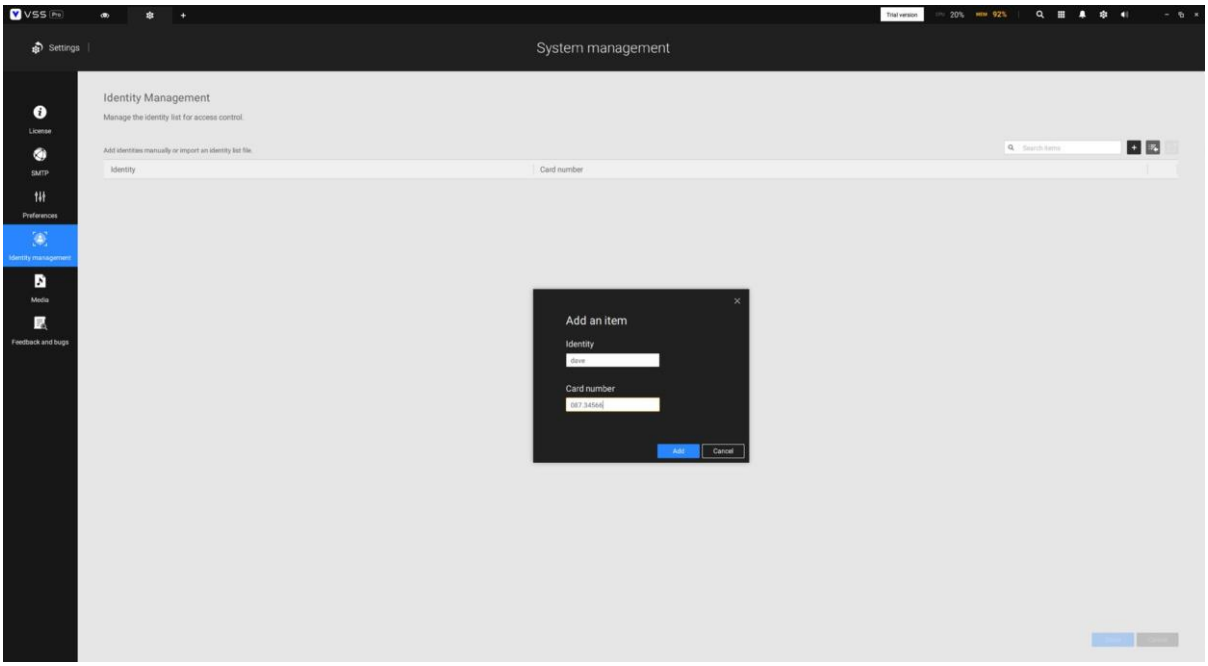


How to configure Identity management?"

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.





An identity table should look like this.