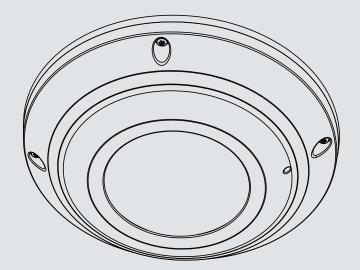


FE8174V Fixed Dome User's Manual

5MP • 360° Surround View • Vandal-proof • PoE



Rev. 1.0

Table of Contents

Overview	
Revision History	4
Read Before Use	5
Package Contents	5
Symbols and Statements in this Document	5
Physical Description	6
Hardware Installation	9
Network Deployment	
Setting up the Network Camera over the Internet	
Software Installation	
Ready to Use	
Accessing the Network Camera	
Using Web Browsers	21
Using RTSP Players	24
Using 3GPP-compatible Mobile Devices	
Using VIVOTEK Recording Software	
Main Page	27
Client Settings	
H.264 / MPEG-4 Media Options	
H.264 / MPEG-4 Protocol Options	
Two way audio	
MP4 Saving Options	40
Local Streaming Buffer Time	40
Configuration	
System > General settings	
System > Homepage layout	
System > Logs	
System > Parameters	
System > Maintenance	
Media > Image	
General settings	52
Day/Night Settings	53
Image settings	54
Exposure	
Privacy mask Pixel Calculator	
Media > Video	
FOV	
Media > Video	63
Stream settings	63
Media > Audio	68
Audio Settings	

Network > General settings	
Network > Streaming protocols	77
Network > QoS (Quality of Service)	
Network > DDNS	
Manual setup	
Network > SNMP (Simple Network Management Protocol)	
Security > User Account	
Security > HTTPS (Hypertext Transfer Protocol over SSL)	
Security > Access List	
Security > IEEE 802.1x	
PTZ > PTZ settings	
Changing the Field of View	
Event > Event settings	
Event	103
Add server	
Add media	
Applications > Motion detection	117
Applications > DI and DO	
Applications > Tampering detection	
Applications > Audio detection	
Applications > VADP (VIVOTEK Application Development Platform)	
Recording > Recording settings	
Local storage > SD card management	
SD card staus	
SD card control	
Local storage > Content management	
Searching and Viewing the Records	131
Search Results	
Appendix	134
URL Commands for the Network Camera	
1. Overview	
2. Style Convention	
Technical Specifications	
Technology License Notice	
MPEG-4 AAC Technology	
MPEG-4 Visual Technology	
AMR-NB Standard	
Electromagnetic Compatibility (EMC)	

Overview

VIVOTEK FE8174/74V is the latest fisheye fixed dome network camera from VIVOTEK, featuring a detailed 5-Megapixel resolution sensor with superb image quality. Equipped with a fisheye lens for 180° panoramic view (wall mount) or 360° surround view (ceiling/floor/table mount) without blind spots, the camera is able to provide coverage of wide, open areas, such as airports, shopping malls, parking lots, retail stores, offices and more.

The FE8174/74V offers various display layouts, including original surround view, panoramic view, and regional view for various mounting applications. With the latest cutting-edge image processing capabilities, hemispherical images captured from the fisheye camera can be converted into conventional rectilinear projection for viewing and analysis. In addition, in both the panoramic as well as regional viewing modes, users can utilize the ultra-smooth ePTZ function to easily zoom in and focus on a region of interest (ROI). The new cutting-edge pixel counter function helps the user to ensure the image quality of a desired area.

As with all VIVOTEK true day/night cameras, the FE8174/74V features a removable IR-cut filter, maintaining clear images 24 hours a day. FE8174V's IP66-rated housing is designed to help the camera body withstand rain and dust and ensures operation under a multitude of harsh weather conditions; additionally, the vandal-proof IK10-rated housing effectively provides robust protection from physical damage. Together with 802.3af compliant PoE, MicroSD/SDHC/SDXC card slot for on-board storage, EN50155 mobile surveillance and iPad applications, the FE8174/4V is indisputably the top choice for constructing a robust surveillance system with the greatest coverage possible.

Revision History

Rev. 1.0: Initial release

Read Before Use

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

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

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

Package Contents

- FE8174V the Network Camera
- Mounting plate / Screwdriver
- 2x Alignment Stickers
- Screws / Dessicant bag / Double-sides tape / Rubber seal plug / Rubber washers
- Power & I/O Cables
- Quick Installation Guide
- Software CD

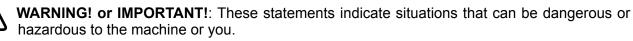
Symbols and Statements in this Document



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

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

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

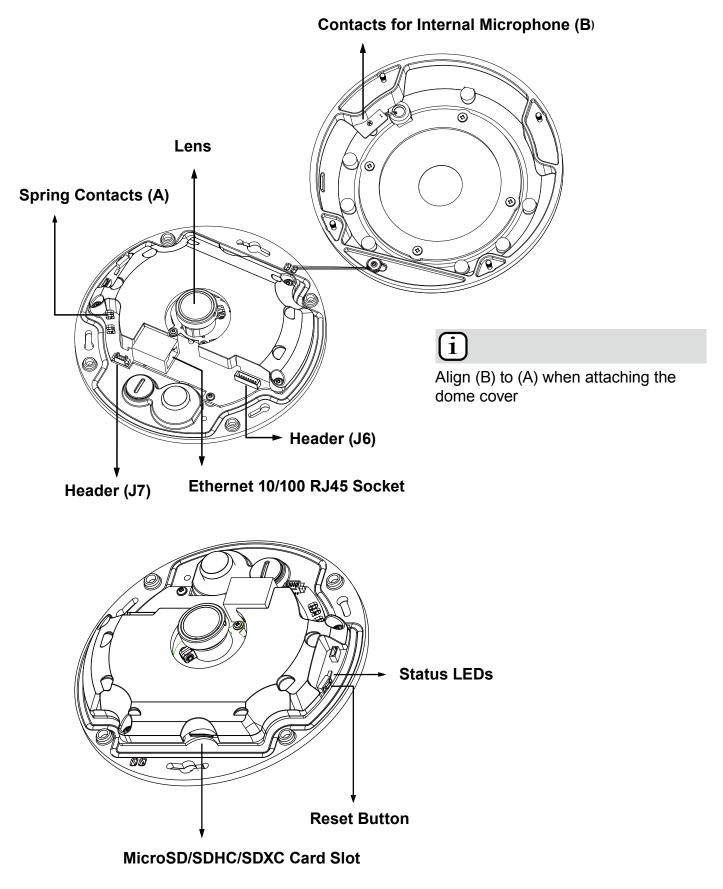




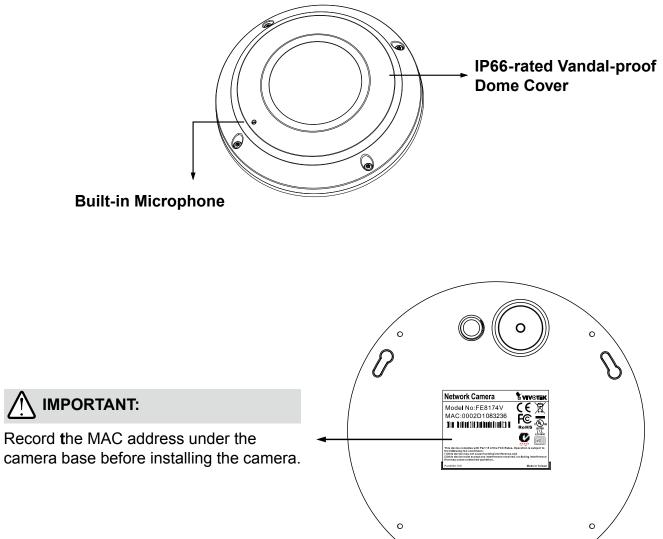
Electrical Hazard: This statement appears when high voltage electrical hazards might occur to an operator.

Physical Description

Inner View



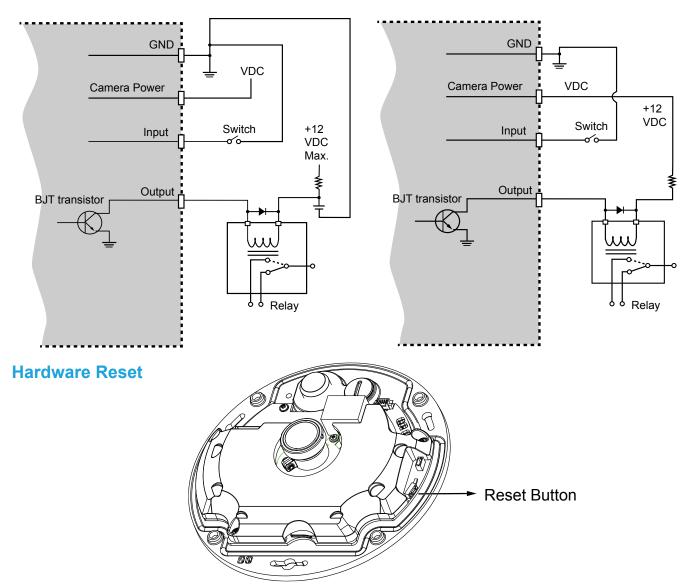
Outer View



Item	LED Status	Description
1	Steady Red	Power on and system booting
	Red LED off	Powered off
2	Steady Red + blinking Green every 1 sec. (Green	Network heartbeat
	LED on for 1 sec and off for another)	
	Steady Red + Green LED off	Network disconnected
3	Blinking Red every 0.15 sec. + Blinking Green	Upgrading firmware
	every 1 sec. (Red LED on for 0.15 sec. and Green	
	LED on for 1 sec. and off for another)	
4	Blinking Red every 0.15 sec. + blinking Green	Restoring defaults
	every 0.15 sec	

DI/DO Diagram

Please refer to the following illustration for the connection method.



The reset button is used to reset the system or restore the factory default settings. Sometimes resetting the system can return the camera to normal operation. If the system problems remain after reset, press the reset button longer to restore the factory settings and install again.

<u>Reset</u>: Press and release the recessed reset button with a straightened paper clip. Wait for the Network Camera to reboot.

<u>Restore</u>: Press and hold the recessed reset button for at least several seconds to restore. Note that all settings will be restored to factory defaults.

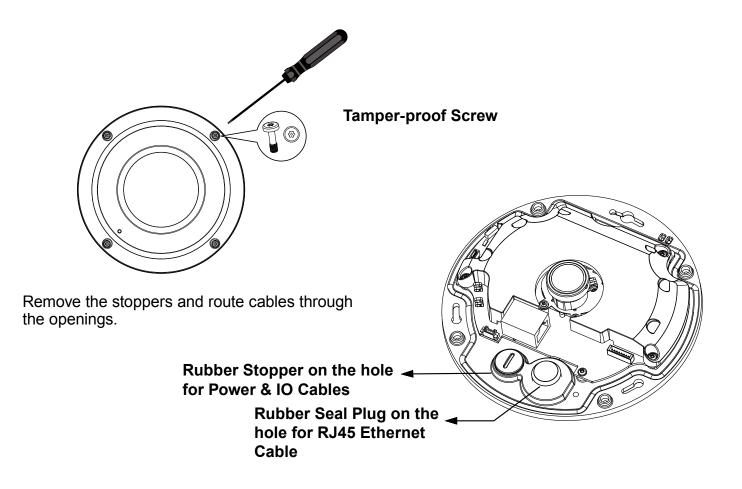
Micro SD/SDHC/SDXC Card Capacity

This network camera is compliant with **Micro SD/SDHC/SDXC 32GB, 64GB**, and other preceding standard SD cards.

Hardware Installation

Opening Dome Cover

First, use the supplied screwdriver to loosen the four screws and detach the dome cover from the camera base. Then, follow the steps below to install the camera to either a ceiling or a wall.



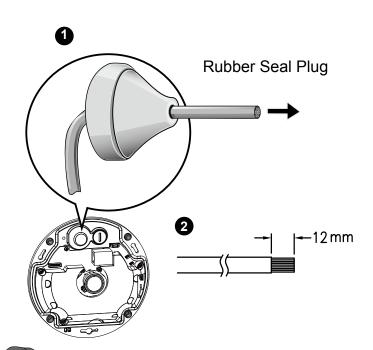
Connecting RJ45 Ethernet Cable

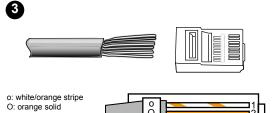
RJ45 Cable Dimension (unit: mm)

Recommended cable gauge: 5 to 8mm

Assembly Steps

- 1. Drill a hole on the rubber seal plug and insert an Ethernet cable through the opening.
- 2. Strip part of the sheath from the Ethernet cable.



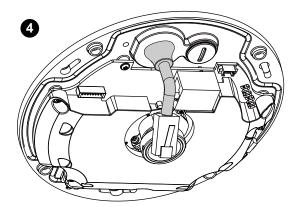


g Bb

- g: white/green stripe B: blue solid b: white/blue stripe G: green solid br: white/brown stripe
- BR: brown solid



3. You will need an RJ45 crimping tool to attach the Ethernet wires to a connector. When done, connect the cable to the camera's Ethernet RJ45 socket.



4. Feed the Ethernet cable from the bottom of the camera and through the hole. Attach the rubber seal plug for water proofing.



2

TH

Connecting DC Power Cable

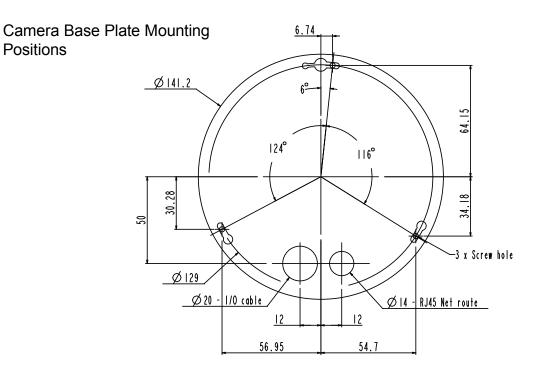
- 1. Add the supplied rubber washer to the cable as shown in the picture.
- 2. Feed the cable from the bottom of the camera and tighten the plastic base for waterproofing.

NOTE:

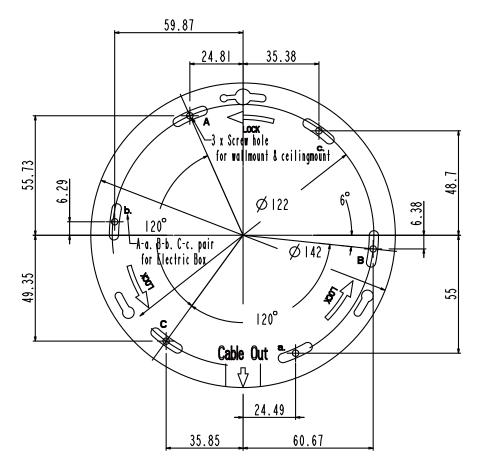
Connect the supplied power & IO cables if your switch does not support PoE.

Mounting Positions

Refer to the diagram on the right for the mounting hole positions and the dimensions of the base plate.



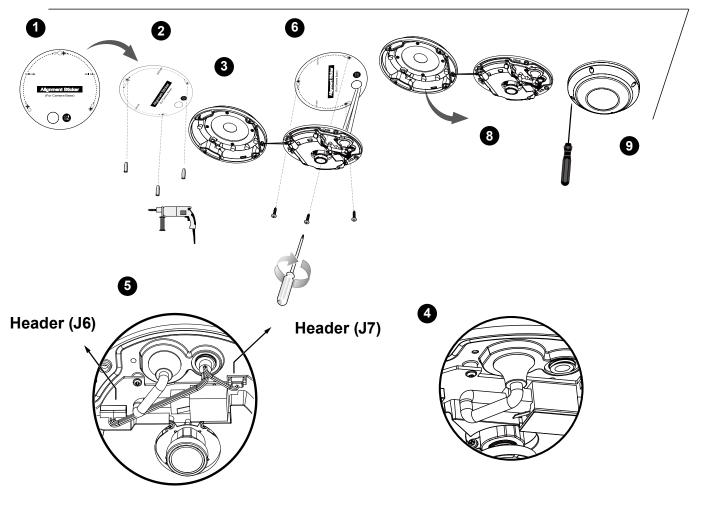
Camera Mounting Plate Mounting Positions



Ceiling/Wall Mount without Mounting Plate

(Choose this mounting type if you want to feed the cables form the bottom of the camera)

- 1. Attach the supplied alignment sticker for camera base to the ceiling/wall.
- 2. Using the three circles on the sticker, drill three pilot holes into the ceiling. Then hammer the three supplied plastic anchors into the holes.
- 3. Drill a cable hole on the ceiling/wall, and feed the cables through the hole.
- 4. Connect the Ethernet cable to the socket.
- 5. Connect the two white header connectors to the J6 and J7 connectors.
- 6. Secure the camera base to the ceiling/wall with three supplied screws.
- 7. You will find a dessicant bag attached to the camera. Replace the dessicant bag included in the camera with the one shipped within the accessory bag.
- 8. Attach the dome cover.
- 9. Secure the four screws with the supplied stardriver. Make sure all camera parts are securely installed.



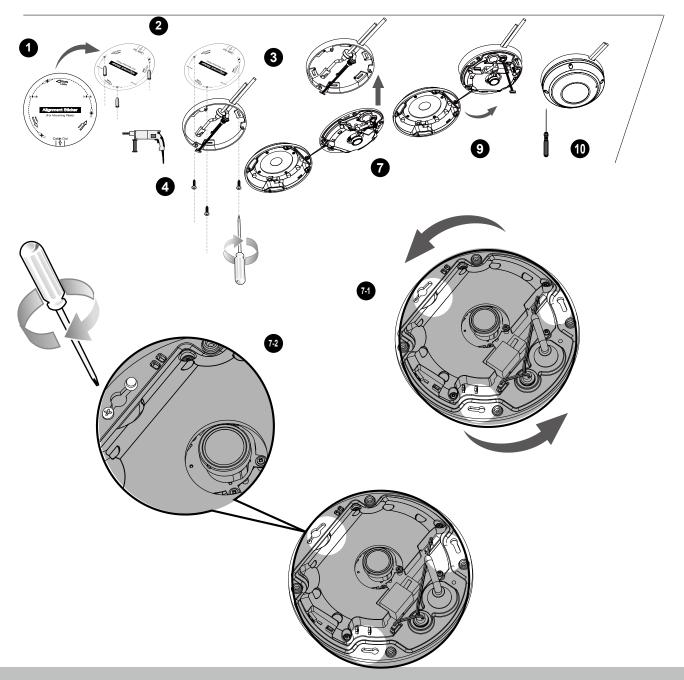
IMPORTANT:

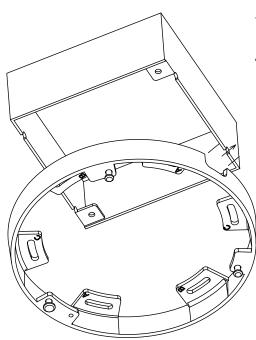
Arrange the cables neatly to avoid getting in the way when the dome cover is attached.

Ceiling/Wall Mount with Mounting Plate

(Choose this mounting type if you would like to feed the cables form the side)

- 1. Attach the supplied alignment sticker for the supplied mounting plate to the ceiling/wall.
- 2. Using the three circles on the sticker, drill three holes into the ceiling. Then hammer the three supplied plastic anchors into the holes.
- 3. Arrange and feed the cables through the side of the mounting plate.
- 4. Secure the mounting plate to the ceiling/wall with three supplied screws.
- 5. Connect the Ethernet cable to the socket.
- 6. Connect two white headers to the J6 and J7 connectors.
- 7. Attach the camera base to the mounting plate and turn counter-clockwise as shown below (Figure 7-1). Then secure the supplied screws to fix the camera base (Figure 7-2).
- 8. You will find a dessicant bag attached to the camera. Replace the dessicant bag with the one shipped within the accessory bag.
- 9. Attach the dome cover.
- 10. Secure the four screws with the supplied stardriver. Make sure all camera parts are securely installed.





You may also use the diagonal holes on the mounting plate, marked as A, B, or C, to install the camera to a U.S. standard 4 in. junction box.

Network Deployment

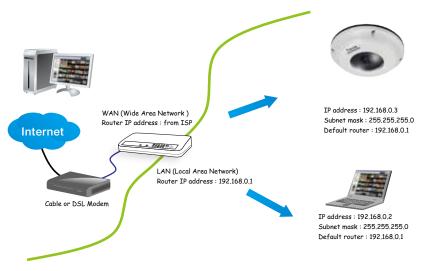
Setting up the Network Camera over the Internet

There are several ways to set up the Network Camera over the Internet. The first way is to set up the Network Camera behind a router. The second way is to utilize a static IP. The third way is to use PPPoE.

Internet connection via a router

Before enabling the access to the Network Camera over the Internet, make sure you have a router and follow the steps below.

1. Connect your Network Camera behind a router, the Internet environment is illustrated below. Regarding how to obtain your IP address, please refer to Software Installation on page 19 for details.



- 2. In this case, if the Local Area Network (LAN) IP address of your Network Camera is 192.168.0.3, please forward the following ports for the Network Camera on the router.
 - Secondary HTTP port: 8080
 - RTSP port: 554
 - RTP port for audio: 5558
 - RTCP port for audio: 5559
 - RTP port for video: 5556
 - RTCP port for video: 5557

If you have changed the port numbers on the Network page, please open the ports accordingly on your router. For information on how to forward ports on the router, please refer to your router's user's manual.

3. Find out the public IP address of your router provided by your ISP (Internet Service Provider). Use the public IP and the secondary HTTP port to access the Network Camera from the Internet. Please refer to Network Type on page 69 for details.

Device	IP Address: internal	IP Address: External Port (Mapped port on the
	port	router)
Public IP of router	122.146.57.120	
LAN IP of router	192.168.2.1	
Camera 1	192.168.2.10:80	122.146.57.120:8000
Camera 2	192.168.2.11:80	122.146.57.120:8001

For example, your router and IP settings may look like this:

Configure the router, virtual server or firewall, so that the router can forward any data coming into a preconfigured port number to a network camera on the private network, and allow data from the camera to be transmitted to the outside of the network over the same path.

From	Forward to
122.146.57.120:8000	192.168.2.10:80
122.146.57.120:8001	192.168.2.11:80

When properly configured, you can access a camera behind the router using the HTTP request as follows: http://122.146.57.120:8000

If you change the port numbers on the Network configuration page, please open the ports accordingly on your router. For example, you can open a management session with your router to configure access through the router to the camera within your local network. Please consult your network administrator for router configuration if you have troubles with the configuration.

For more information with network configuration options (such as that of streaming ports), please refer to Configuration > Network Settings. VIVOTEK also provides the automatic port forwarding feature as an NAT traversal function with the precondition that your router must support the UPnP port forwarding feature.

Network > General settings			
System	Network type Port		
Media	. LAN		
Network	Get P address automatically		
General settings	Use fixed P address Enable UPnP presentation		
Streaming protocols			
DONS	[2] Enable UPnP port forwarding		
QoS	PPPoE		
SNMP	Enable Pv6		
Security	The device is configuring now. Your prowser will reconnect IPv6 informu to http://192.168.4.140.80/		
PTZ	Manually If the connection fails, please manually enter the above P address in your browser.		
Event	Save		

Internet connection with static IP

Choose this connection type if you are required to use a static IP for the Network Camera. Please refer to LAN configuration on page 69 for details.

Internet connection via PPPoE (Point-to-Point over Ethernet)

Choose this connection type if you are connected to the Internet via a DSL Line. Please refer to PPPoE on page 90 for details.

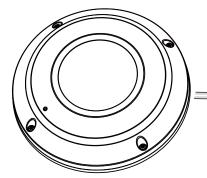
Set up the Network Camera through Power over Ethernet (PoE)

When using a PoE-enabled switch

The Network Camera is PoE-compliant, allowing transmission of power and data via a single Ethernet cable. Follow the below illustration to connect the Network Camera to a PoE-enabled switch via an Ethernet cable.

<u>7</u>

- 1. The camera is only to be connected to PoE networks without routing to outside plants.
- 2. For PoE connection, use only UL listed I.T.E. with PoE output.



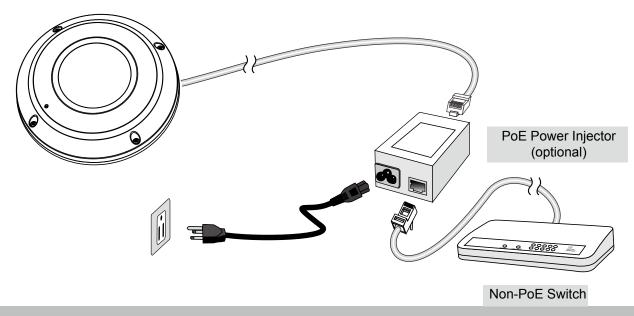
Power + Data Transmission



PoE Switch

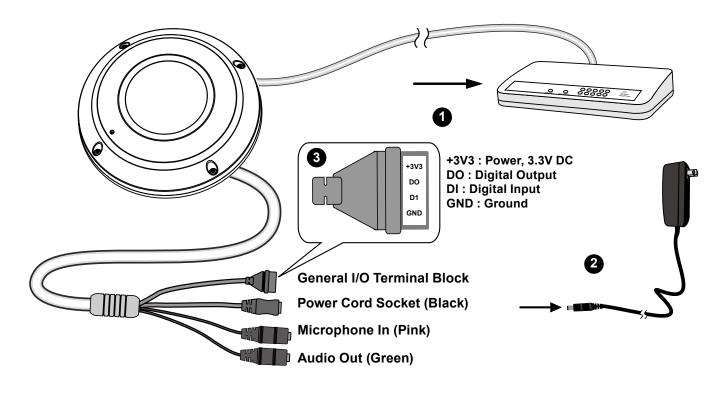
When using a non-PoE switch

If your switch/router does not support PoE, use a PoE power injector (optional) to connect between the Network Camera and a non-PoE switch.



General Connection (without PoE)

- 1. If you have external DI devices, make the connection from general I/O terminal block.
- 2. Ethernet, power and IO cables are user-supplied.
- 3. Connect DC power cord to a DC Adapter, and then to a power outlet.



NOTE:

The power adapter should comply with L.P.S. regulations featuring O/P: 12V DC, 1.5A min.

Software Installation

Installation Wizard 2 (IW2), free-bundled software included on the product CD, helps you set up your Network Camera on the LAN.

1. Install IW2 under the Software Utility directory from the software CD. Double click the IW2 shortcut on your desktop to launch the program.



2. The program will conduct an analysis of your network environment. After your network environment is analyzed, please click **Next** to continue the program.

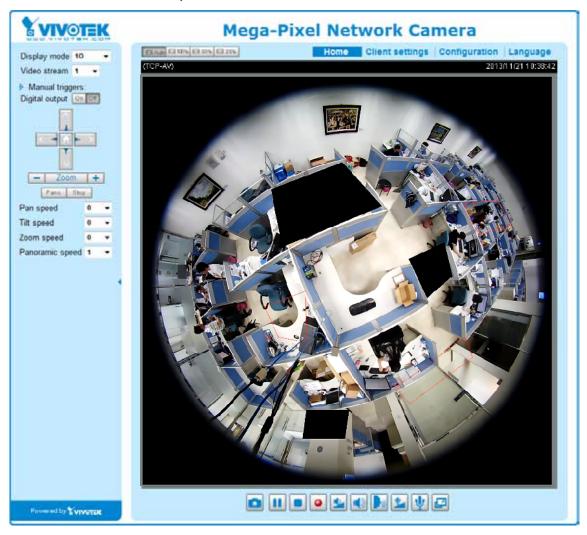
🖷 Installation. Winard 2 – Referenk Environment Analysis 🛛 🔀	🖣 Testelletion Winord 3 - Network Type
Installation Wizard 2	Installation Wizard 2
The wizard is analyzing your network environment. Please walt a moment.	Your network environment was analyzed as below. Private DHCP
	Cable 1955 modem Router K
Ext	Let Net

- 3. The program will search for all VIVOTEK network devices on the same LAN.
- 4. After a brief search, the main installer window will pop up. Double-click on the MAC address that matches the one printed on the camera label or the S/N number on the package box label to open a browser management session with the Network Camera.

	Installation Wizard 2	2	×
Network CameraModel No: FE8174VMAC: 0002D1083236Marce complexityMarce complexity <th>Device Selectio Select a device to Smart Setup Refresh Devices</th> <th>installa</th> <th>tion Wizard 2</th>	Device Selectio Select a device to Smart Setup Refresh Devices	installa	tion Wizard 2
		Prease check the MAC and model name in the product label of your device first. Then, you can start to link to your device and show the main screen by double clicking the item in the above selection list. If you are not able to find your device in the above selection list, please make sure all cables are properly connected to your device and then click on the "Refresh Devices" button.	Mac.coop21XXXXX Literative for the second se

Ready to Use

- 1. A browser session with the Network Camera should prompt as shown below.
- 2. You should be able to see live video from your camera. You may also install the 32-channel recording software from the software CD in a deployment consisting of multiple cameras. For its installation details, please refer to its related documents.



NOTE:

If you encounter problems with displaying live view or the onscreen plug-in control, you may try to remove the plug-ins that might have been installed on your computer. Remove the following folder: C:\Program Files (x86)\Camera Stream Controller\.

Accessing the Network Camera

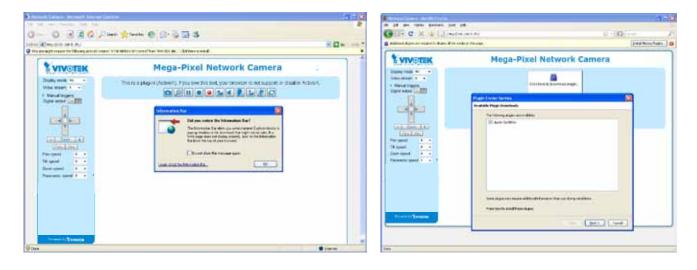
This chapter explains how to access the Network Camera through web browsers, RTSP players, 3GPP-compatible mobile devices, and VIVOTEK recording software.

Using Web Browsers

- Currently the Network Camera utilizes 32-bit ActiveX plugin. You CAN NOT open a management/view session with the camera using a 64-bit IE browser.
- If you encounter this problem, try execute the lexplore.exe program from C:\Windows\ SysWOW64. A 32-bit version of IE browser will be installed.
- On Windows 7, the 32-bit explorer browser can be accessed from here: C:\Program Files (x86)\Internet Explorer\iexplore.exe

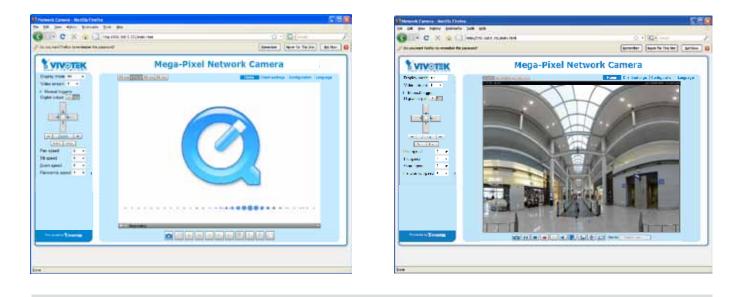
Use Installation Wizard 2 (IW2) to access to the Network Cameras on the LAN.

- If your network environment is not a LAN, follow these steps to access the Network Camera:
- 1. Launch your web browser (e.g., Microsoft[®] Internet Explorer, Mozilla Firefox, or Netscape).
- 2. Enter the IP address of the Network Camera in the address field. Press Enter.
- 3. The live video will be displayed in your web browser.
- 4. If it is the first time installing the VIVOTEK network camera, an information bar will prompt as shown below. Follow the instructions to install the required plug-in on your computer.





For **Mozilla Firefox** users, your browser will use **Quick Time** to stream live video. If you do not have Quick Time on your computer, please download Quick Time from Apple Inc's website, and then launch your web browser.

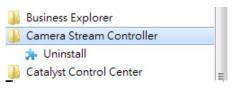




The onscreen Java control can malfunction under the following situations:

A PC connects to different cameras that are using the same IP address (or the same camera running different firmware versions). Removing your browser cookies will solve this problem.

 In the event of plug-in compatibility issues, you may try to uninstall the plug-in that was previously installed.





- 1. By default, your Network Camera is not password-protected. To prevent unauthorized access, it is highly recommended to configure a password for your camera later. *For more information about how to enable password protection, please refer to Security on page 88*.
- 2. If you see a dialogue box indicating that your security settings prohibit running ActiveX Controls®, please enable ActiveX Controls for your browser.

To enable the ActiveX[®] Controls for your browser:

2-1. Choose Tools > Internet Options > Security > Custom Level.

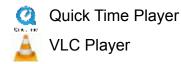
2-2. Look for Download signed ActiveX[®] controls; select Enable or Prompt. Click **OK**.

General Security Privacy Content Connections Programs Advanced
Select a Web content zone to specify its security settings.
Internet Local intranet Trusted sites
Internet This zone contains all Web sites you haven't placed in other zones
Security level for this zone
Custom Custom settings. - To change the settings, click Custom Level. - To use the recommended settings, click Default Level.
Custom Level Default Level
OK Cancel Apply
Security Settings
Security Settings ?X
Settings:
Settings: ActiveX controls and plug-ins Download signed ActiveX controls
Settings:
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt Download unsigned ActiveX controls
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt Download unsigned ActiveX controls Disable Enable Prompt
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt Download unsigned ActiveX controls Disable Enable Prompt Initialize and script ActiveX controls not marked as safe
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt Download unsigned ActiveX controls Disable Enable Prompt
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt Download unsigned ActiveX controls Disable Enable Prompt Initialize and script ActiveX controls not marked as safe Disable Enable Prompt Prompt
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt Download unsigned ActiveX controls Disable Enable Prompt Initialize and script ActiveX controls not marked as safe Disable Enable Disable Enable Disable Enable
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt Download unsigned ActiveX controls Disable Enable Prompt Initialize and script ActiveX controls not marked as safe Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Disable Enable Prompt Prompt Prompt Prompt Prompt
Settings: ActiveX controls and plug-ins Download signed ActiveX controls Disable Enable Prompt Disable Enable Prompt Initialize and script ActiveX controls not marked as safe Disable Enable Prompt Disable Enable Disable Enable Normation of the set

2-3. Refresh your web browser, then install the ActiveX[®] control. Follow the instructions to complete installation.

Using RTSP Players

To view the H.264/MPEG-4 streaming media using RTSP players, you can use one of the following players that support RTSP streaming.



- 1. Launch the RTSP player.
- 2. Choose File > Open URL. A URL dialog box will prompt.
- The address format is rtsp://<ip address>:<rtsp port>/<RTSP streaming access name for stream1 to stream4>

As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 78. For example:

Open URL		\mathbf{X}
Enter an Internet URL to op	en:	
rtsp://192.168.5.151:554/	ive.sdp	▼
		OK Cancel

4. The live video will be displayed in your player. For more information on how to configure the RTSP access name, please refer to RTSP Streaming on page 78 for details.



The RTSP players will show the original circular-shape image. You can access the Regional views via the ST7501 or VAST software. See page 79 for an example.

Using 3GPP-compatible Mobile Devices

To view the streaming media through 3GPP-compatible mobile devices, make sure the Network Camera can be accessed over the Internet. For more information on how to set up the Network Camera over the Internet, please refer to Setup the Network Camera over the Internet on page 15.

To utilize this feature, please check the following settings on your Network Camera:

- 1. Because most players on 3GPP mobile phones do not support RTSP authentication, make sure the authentication mode of RTSP streaming is set to disable. For more information, please refer to RTSP Streaming on page 78.
- 2. As the the bandwidth on 3G networks is limited, you will not be able to use a large video size. Please set the video and audio streaming parameters as listed below. For more information, please refer to Stream settings on page 63.

Video Mode	MPEG-4
Frame size	176 x 144
Maximum frame rate	5 fps
Intra frame period	1S
Video quality (Constant bit rate)	40kbps
Audio type (GSM-AMR)	12.2kbps

- 3. As most ISPs and players only allow RTSP streaming through port number 554, please set the RTSP port to 554. For more information, please refer to RTSP Streaming on page 78.
- 4. Launch the player on the 3GPP-compatible mobile devices (e.g., Real Player).
- Type the following URL commands in the URL field. The address format is rtsp://<public ip address of your camera>:<rtsp port>/<RTSP streaming access name for stream 3>. For example:

Open URL		×
Enter an Internet URL to op	en:	
rtsp://192.168.5.151:554/	live.sdp	×
		OK Cancel

Using VIVOTEK Recording Software

The product software CD also contains recording software, allowing simultaneous monitoring and video recording for multiple Network Cameras. Please install the recording software; then launch the program to add the Network Camera to the Channel list. For detailed information about how to use the recording software, please refer to the user's manual of the software or download it from http://www.vivotek.com.



Main Page

This chapter explains the screen elements on the main page. It is composed of the following sections: VIVOTEK INC. Logo, Host Name, Camera Control Area, Configuration Area, and Live Video Window.



VIVOTEK INC. Logo

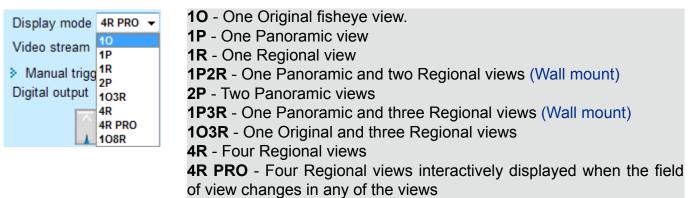
Click this logo to visit the VIVOTEK website.

Host Name

The host name can be customized to fit your needs. For more information, please refer to System > General Settings on page 42.

Camera Control Area

Display mode: This is a brand new configuration menu exclusively designed for Fisheye cameras. Due to the fisheye lens' wide coverage of 180° hemispheric and 360° panoramic views and to manipulate the details within, the following display modes are provided:



108R - One Original and eight Regional views

* Most display modes are available in the Ceiling mount type.

* See following discussions for detailed explanation of these modes. If selected, the Wall mount type provides another two distinctive modes.

The Local dewarp function is designed for use with 3rd-party software that did not implement the dewarp plug-ins. A video stream can be dewarped on the camera into a regional or panoramic view before being sent to the client side. However, since the video has already been dewarped into a more viewable rectilinear view, you can not exert PTZ control or change the view angle on the client computer.

When using the Local dewarp, you should first configure the view angle of a regional view in the PTZ > PTZ settings window.

Below are the appearances of the control panel when the Local dewarp function is enabled or disabled. The **PTZ panel** and the **Display mode** menu disappear when a video stream is using the Local dewarp function. See page 65 for more information.

Local dewarp (on camera)	Dewarp by client-side plug-ins	Dewarp by client-side plug-ins			
Video stream I Image: Image	Display mode 10 Video stream 1 Manual triggers: Digital output Pano. Stop Pan speed 0 Tilt speed 0 Zoom speed 0 Panoramic speed 1	Display mode 10 Video stream 1P 1P 1R 2P 103R 4R 4R PR0 108R 118 speed 108 200m speed 108 200m speed 108			
Powered by YVIVOTEK	Powered by YIVOTEK	Powered by YVVOTEK			

10 (Original) Display mode:

When mounted on a ceiling, the fisheye camera can cover an approximately 50 m² of surveillance area (hung at a height of approximately 3 meters), while still keeping details in videos with recognizable facial features of people trafficking through the area.

The 1O view is especially adequate for taking an overview glimpse of surveillance area with a ceiling mount camera.



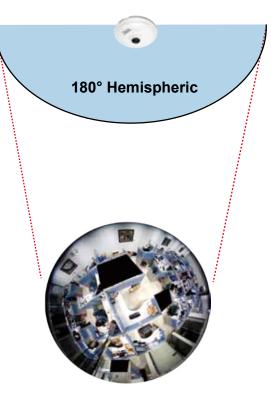
With image correction firmware algorithms, the hemispheric image is transformed into a rectilinear stripe in the 1P display mode. Viewers can use the PTZ panel or simply use mouse control to quickly move through the 360° panoramic view. (Mouse control on the Panoramic view is available with the Ceiling mount type.)

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



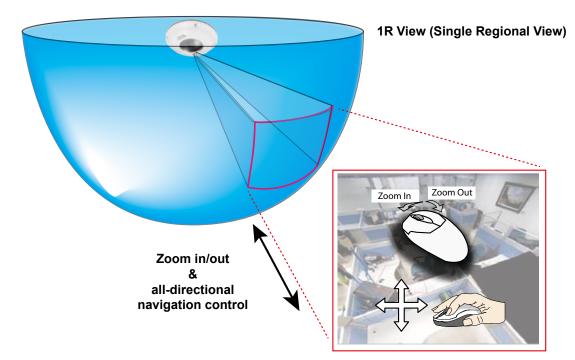
If the Local dewarp mode is selected for a video stream, the mouse control on the screen will be disabled. For example, if Local dewarp "1R" mode is selected (see description on the next page), its view angle will not be configurable using the mouse control.

10 View (Original View)



1R (Single Regional) Display mode:

The 1R mode provides access to one image section within the hemisphere. You can zoom in or out (using the mouse wheel or PTZ panel) or travel to other areas in the hemisphere using mouse clicks and swipes. A single click on a particular object can bring the object to the center of your view window. Click and hold down the left mouse button, and you can swipe the view both horizontally and vertically.



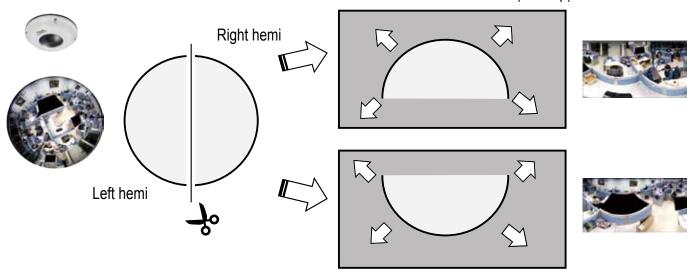
2P (Dual Panoramic View) Display mode:

Similar to 1P, the 2P display mode provides simultaneous access to both the left and right sections of a hemisphere. Both panoramic views are corrected into a more viewable dewarped image. Viewers can use a mouse click and swipe to quickly scroll horizontally through the surveillance area.

* Note that the dividing line falls approximately on center of the VIVOTEK logo.



Converted to rectilinear view (Dewarp)

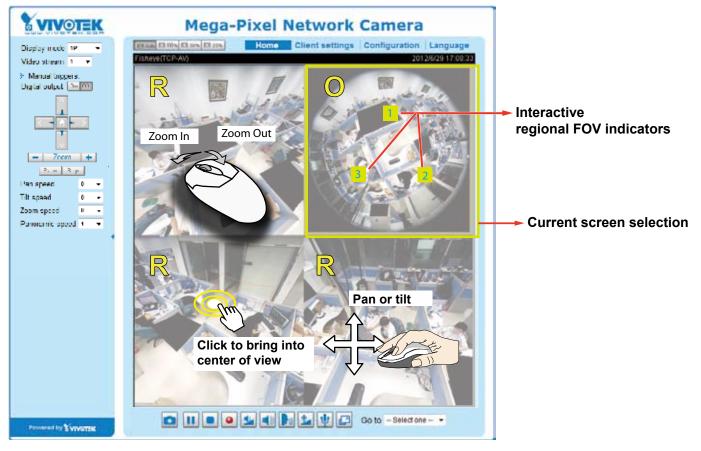


103R (One Original & Three Regional) Display mode:

The 1O3R mode provides access to multiple live view sections within the hemisphere and the reference to their relative positions on an Original circular view. The FOV indicators ($#1 \sim #3$) interact with your current operation as you may zoom in/out or move the live view window to a different place.

You can zoom in or out or travel to other areas within the hemisphere using identical methods as previously described in the 1R mode.

You can also change the locations of Regional views by dragging the FOV indicators on the "Original" circular view.



103R (Original & Regional) Mode Screen Control



In a Regional view displaying 100% of video feed (via the Resize buttons - see page 34), your mouse wheel can be used to scroll the view window vertically before you click on a live image. After you click on the live image, the mouse wheel becomes the zoom in/out tool.

4R (Four Regional) Display mode:

The view control and look and feel are identical to that as described in the 1O3R mode except the absence of the Original circular view.

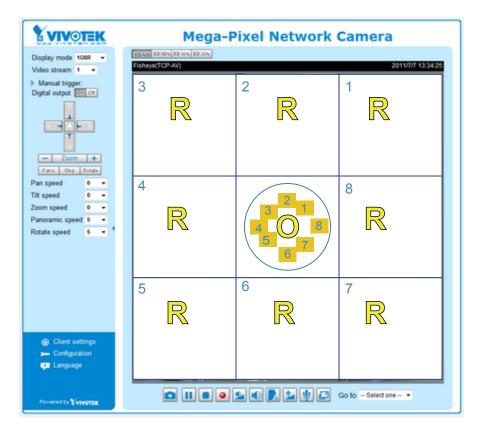
4R PRO (Four Regional Proactive) Display mode:

The 4R PRO mode is similar to the 4R mode except that the quad view windows consecutively rotate in correspondence to the change of view area in one window. Note that zoom in/out and tilt control is not available in this mode.

108R (One Original and Eight Regional) Display mode:

The view control and look and feel are identical to that as described in the 1O3R mode.

Note that if you change the position of a view in hemisphere, e.g., #3 window, you may lose the configuration change by switching to another display mode. The live view window does not automatically save your view section layout.



1P2R (One Panoramic and Two Regional) Display mode: **1P3R** (One Panoramic and Three Regional) Display mode:

These two modes are only available with the **Wall Mount type**! The Mount type configuration is found in **Configuration > Media > Image > General Settings**. Please refer to page 52 for details.

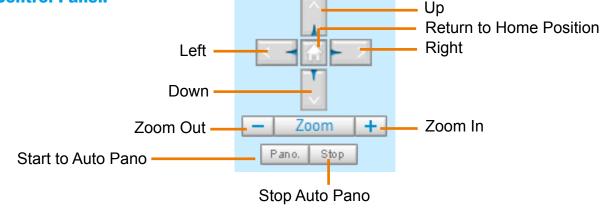
The view control in these two modes is identical to that as described in the 1O3R mode.

<u>Video Stream</u>: This Network Cmera supports multiple streams (stream $#1 \sim #3$) simultaneously. You can select any one of them for live viewing. For more information about multiple streams, please refer to page 63 for detailed information.

<u>Manual Trigger</u>: Click to manually enable or disable an event trigger. Please configure an event setting before enabling this function. A total of 3 or 4 event settings can be configured. For more information about event setting, please refer to page 103. If you want to hide this item on the homepage, please go to the **System > Homepage Layout > General settings > Customized button** to deselect the "show manual trigger button" checkbox.

Digital Output: Click to turn the digital output device on or off.

PTZ Control Panel:



The PTZ panel will not appear if you configure a video stream to be using the "Local dewarp" feature. To change the shooting direction of a locally-dewarped regional view, please refer to page 101 "PTZ panel" for details.

<u>Pano.</u>: Click this button to start the automated circular rotation through a regional view (360° continuous rotation). Note that this function does not apply in a Panoramic view because a Panoramic view already

Pan speed	Tilt speed	Zoom speed	Panoramic speed	Rotate speed	
-5	-5	-5	-	-	Slower
-4	-4	-4	-	-	
-3	-3	-3	-	-	
-2	-2	-2	-	-	
-1	-1	-1	-	-	
0	0	0	0	0	
1	1	1	1	1	
2	2	2	2	2	
3	3	3	3	3	
4	4	4	4	4	
5	5	5	5	5	Faster

shows the full coverage.

Stop: Click this button to stop the Auto Pano and Auto Rotate functions.

Pan /Tilt /Zoom /Panoramic/Rotate speed: Adjust the speed of these controls when exerted:



Unlike previous fisheye cameras, the PTZ preset positions function has been cancelled on this model. Therefore, the Rotate function is also unavailable.

Configuration Area

<u>Client Settings</u>: Click this button to access the client setting page. For more information, please refer to Client Settings on page 39.

<u>Configuration</u>: Click this button to access more of the configuration options provided with the Network Camera. It is suggested that a password is applied to the Network Camera so that only the administrator can configure the Network Camera. For more information, please refer to the description for the Configuration menus on page 41.

<u>Language</u>: Click this button to choose a language for the user interface. Language options are available in: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文. You can also change a language on the Configuration page; please refer to page 41.

Hide Button

You can click the hide button to hide the control panel or display the control panel.

Resize Buttons

E Auto E 100% E 50% E 25% .

Click the Auto button, the video cell will resize automatically to fit the monitor. Click 100% is to display the original homepage size. Click 50% is to resize the homepage to 50% of its original size. Click 25% is to resize the homepage to 25% of its original size.

Live Video Window

■ The following window is displayed when the video mode is set to H.264 / MPEG-4:



<u>Video Title</u>: The video title can be configured. For more information, please refer to Video settings on page 63.

<u>H.264 / MPEG-4 Protocol and Media Options</u>: The transmission protocol (TCP or UDP, etc.)and media options for H.264 / MPEG-4 video streaming. For further configuration, please refer to Client Settings on page 39.

<u>Time</u>: Display the current time. For further configuration, please refer to Media > Image > Genral settings on page 52.

<u>Title and Time</u>: The video title and time can be stamped on the streaming video. For further configuration, please refer to Media > Image > Genral settings on page 52.

<u>Video and Audio Control Buttons</u>: Depending on the Network Camera model and Network Camera configuration, some buttons may not be available.

Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Pause: Pause the transmission of the streaming media. The button becomes the	Resume button
er clicking the Pause button.	

	Stop:	Stop	the	transmissi	on of	the	streaming	media.	Click the	Resume	button	to	continue
tran	ismissi	on.											

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 40 for details.

Volume: When the Mute function is not activated, move the slider bar to adjust the volume on the local computer.

Mute: Turn off the volume on the local computer. The button becomes the Mutio On button after clicking the Mute button.

<u>Talk</u>: Click this button to talk to people around the Network Camera. Audio will project from the external speaker connected to the Network Camera. Click this button again to end talking transmission.

Mic Volume: When the W Mute function is not activated, move the slider bar to adjust the microphone volume on the local computer. Note that inernal microphone is mounted on the dome cover.

W Mute: Turn off the Mic volume on the local computer. The button becomes the Mic On button after clicking the Mute button.

Full Screen: Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode.

■ The following window is displayed when the video mode is set to MJPEG:



<u>Video Title</u>: The video title can be configured. For more information, please refer to Media > Image on page 52.

<u>Time</u>: Display the current time. For more information, please refer to Media > Image on page 52.

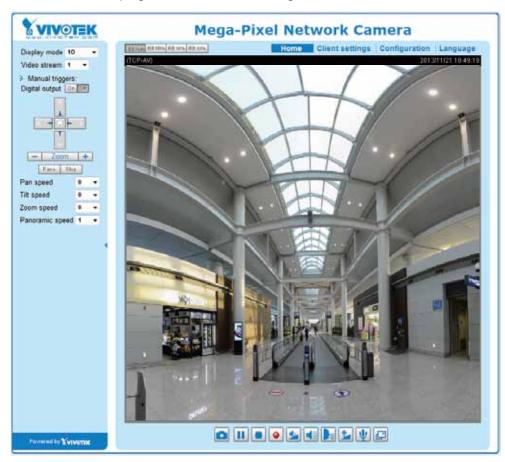
<u>Title and Time</u>: Video title and time can be stamped on the streaming video. For more information, please refer to Media > Image on page 52.

<u>Video Control Buttons</u>: Depending on the camera model and your current configuration, some buttons may not be available.

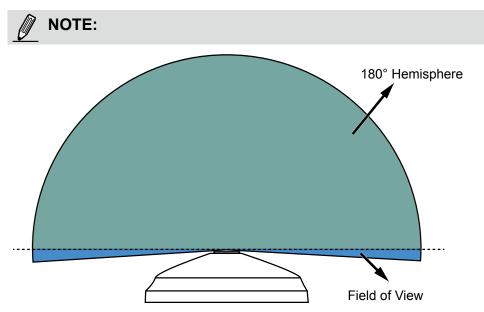
Snapshot: Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose **Save Picture As** to save it in JPEG (*.jpg) or BMP (*.bmp) format.

Start MP4 Recording: Click this button to record video clips in MP4 file format to your computer. Press the Stop MP4 Recording button to end recording. When you exit the web browser, video recording stops accordingly. To specify the storage destination and file name, please refer to MP4 Saving Options on page 40 for details.

Full Screen: Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode.



Please refer to page 101 for PTZ settings.



- 1. Edges of a fisheye circular view will be slightly cropped because the fisheye lens FOV is actually larger than the sensor can take.
- 2. The camera lens' angle of view is larger than 180°. Therefore, the camera's circular view is actually larger than a 180° hemisphere.
- 3. Since the field of view is larger than a hemisphere, the top edge of dome cover (the round opening where the lens is revealed) may appear as a white circle around a circular view.
- 4. When using the dewarped modes, e.g., the Regional and Panoramic views, the firmware will not capture the far edges of the FOV which extends beyond the 180° hemisphere.



- 1. The onscreen Java control can malfunction under the following situations: A PC connects to different cameras that are using the same IP address (or the same camera running different firmware versions). Removing your browser cookies will solve this problem.
- 2. If you encounter problems with displaying the configuration menus or UI items, try disable the Compatibility View on IE8 or IE9.



You may also press the F12 key to open the developer tools utility, and then change the Browser Mode to the genuine IE8 or IE9 mode.

A>	
File Find Disable View Images Cache Tools Validate	Browser Mode: IE9 Document Mode: IE9 standards
HTML CSS Console Script Profiler Network	Internet Explorer 7
	Internet Explorer 8
<pre>!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 "</pre>	Internet Explorer 9 Compatibility View

Client Settings

This chapter explains how to select the stream transmission mode and saving options on the local computer. When completed with the settings on this page, click **Save** on the page bottom to enable the settings.

H.264 / MPEG-4 Media Options

 H.264/MPEG-4 Media Options
♥ Video and Audio
🔿 Video Only
O Audio Only

Select to stream video or audio data or both. This is enabled only when the video mode is set to H.264 or MPEG-4.

H.264 / MPEG-4 Protocol Options

 H.264/MPEG-4 Protocol Options	1
O UDP Unicast	
O UDP Multicast	
⊙ TCP	
○ HTTP	
	L

Depending on your network environment, there are four options with the transmission protocols with H.264 or MPEG-4 streaming:

<u>UDP unicast</u>: This protocol allows for more real-time audio and video streams. However, network packets may be lost due to network burst traffic and images may be broken. Activate UDP connection when occasions require time-sensitive responses and the video quality is less important. Note that each unicast client connecting to the server takes up additional bandwidth and the Network Camera allows up to ten simultaneous accesses.

<u>UDP multicast</u>: This protocol allows multicast-enabled routers to forward network packets to all clients requesting streaming media. This helps to reduce the network transmission load of the Network Camera while serving multiple clients at the same time. Note that to utilize this feature, the Network Camera must be configured to enable multicast streaming at the same time. For more information, please refer to RTSP Streaming on page 78.

<u>TCP</u>: This protocol guarantees the complete delivery of streaming data and thus provides better video quality. The downside of this protocol is that its real-time effect is not as good as that of using the UDP protocol.

<u>HTTP</u>: This protocol allows the same quality as TCP protocol without needing to open specific ports for streaming under some network environments. Users behind a firewall can utilize this protocol to allow camera's streaming data to pass through.

Two way audio

Γ	Two way audio	٦
	Half-duplex	
	Full-duplex	

Select one of the checkboxes to configure the two way audio into the half- or full-duplex mode.

MP4 Saving Options

Γ	MP4 saving opt	ions	
	Folder:	D:\Record3	Browse
	File name prefix:	CLIP]
	🔽 Add date and t	time suffix to file name	

Users can record live video as they are watching it by clicking the end "Start MP4 Recording" button on the main page. Here, you can specify the storage destination and file name.

Folder: Specify a storage destination for the recorded video files.

File name prefix: Enter the text that will be appended to the front of the video file name.

Add date and time suffix to the file name: Select this option to append the date and time to the end of the file name.



Local Streaming Buffer Time

Γ	Local	Streaming Buffer Time
	0	Millisecond
	Save	

Due to possible occurrences of unsteady network transmission, live streaming may lag and not be very smoothly. If you enable this option, the live streaming will be stored on the client PC's cache memory for a few seconds before being played on the client computer's live view window. This helps produce a smoothlier live streaming. If you enter a vlue of 3,000 milliseconds, the streaming will delay for 3 seconds.

Configuration

Click **Configuration** on the main page to enter the camera setting pages. Note that only Administrators can access the configuration page.

VIVOTEK provides an easy-to-use user interface that helps you set up your network camera with minimal effort. In order to simplify the user interface, detailed information will be hidden unless you click on the function item. When you click on the first sub-item, the detailed information for the first sub-item will be displayed; when you click on the second sub-item, the detailed information for the second sub-item will be displayed and that of the first sub-item will be hidden.

The following is the interface of the main page:

VIVOTEK					
WWW.VIVOTER.COM		Home	Client settings	Configuration	Language
	System > General settings				
System	System		uala Lumpur, Singapore, Taipei 💌		
General settings	Host name:	Mega-Pit	kel Network Camera		
Homepage layout Logs	Turn off the LED indicator		onq, Kuala Lumpur, Sinqapore, Taipei 💌		
Parameters	System time			umpur, Sinqapore, Taipei 💌	
Maintenance	Time zone: GMT+08:00 Beijing, Chongging,	, Hong Kong, I	Kuala Lumpur, Sinqap	ore, Taipei 💌	
Media Network	Note: You can upload your daylight savin value.	g time rules o	n <u>Maintenance</u> page		
Network	Keep current date and time				
Security	K Keep current date and time Synchronize with computer time Manual 				
РТΖ	Manual				
Event	Automatic				
Applications	-Configuration List			S	ave
Recording					
Local storage					
Version: 0100a	- Firmware Version				

Each function on the configuration list will be explained in the following sections.

The Navigation Area provides access to all different views from the **Home** page (for live viewing), **Configuration** page, and multi-language selection.

System

System > General settings

This section explains how to configure the basic settings for the Network Camera, such as the host name and system time. It is composed of the following two columns: System and System Time.

Mega-Pixel Network Camera

<u>Host name</u>: Enter a desired name for the Network Camera. The name will be displayed at the top center of the main page.

Turn off the LED indicator: Click to disable the onboard LEDs.

System time

ime zone:	GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei 💌
Note: You default va	can upload your daylight saving time rules on <u>Maintenance</u> page or use the camera lue.
Keep cu	rrent date and time
Synchro	nize with computer time
🖱 Manual	
Automat	ic

<u>Time zone</u> : Select the appropriate time zone from the list. If you want to upload Daylight Savings Time rules, please refer to **System > Maintenance > Import/ Export files** on page 49 for details.

<u>Keep current date and time</u>: Select this option to preserve the current date and time of the Network Camera. The Network Camera's internal real-time clock maintains the date and time even when the power of the system is turned off.

<u>Synchronize with computer time</u>: Select this option to synchronize the date and time of the Network Camera with the local computer. The read-only date and time of the PC is displayed as updated.

<u>Manual</u>: The administrator can enter the date and time manually. Note that the date and time format are [yyyy/mm/dd] and [hh:mm:ss].

<u>Automatic</u>: The Network Time Protocol is a protocol which synchronizes computer clocks by periodically querying an NTP Server.

<u>NTP server</u>: Assign the IP address or domain name of the time-server. Leaving the text box blank connects the Network Camera to the default time servers.

<u>Update interval</u>: Select to update the time using the NTP server on an hourly, daily, weekly, or monthly basis.

When finished with the settings on this page, click **Save** at the bottom of the page to enable the settings.

System > Homepage layout

This section explains how to set up your own customized homepage layout.

General settings

This column shows the settings of your hompage layout. You can manually select the background and font colors in Theme Options (the second tab on this page). The settings will be displayed automatically in this Preview field. The following shows the homepage using the default settings:



■ Hide Powered by VIVOTEK: If you check this item, it will be removed from the homepage.

Logo graph

Here you can change the logo at the top of your homepage.

	Logo graph		
	A customized logo (Gif, JPG o 160x50 pixels to replace the p	or PNG) can be uploaded for main page. It will be resize previous logo.	ed to
(Default	⊙ Custom	
			Browse
L	ogo link: http://www.vivotek.c	com	

Follow the steps below to upload a new logo:

- 1. Click **Custom** and the Browse field will appear.
- 2. Select a logo from your files.
- 3. Click **Upload** to replace the existing logo with a new one.
- 4. Enter a website link if necessary.
- 5. Click **Save** to enable the settings.

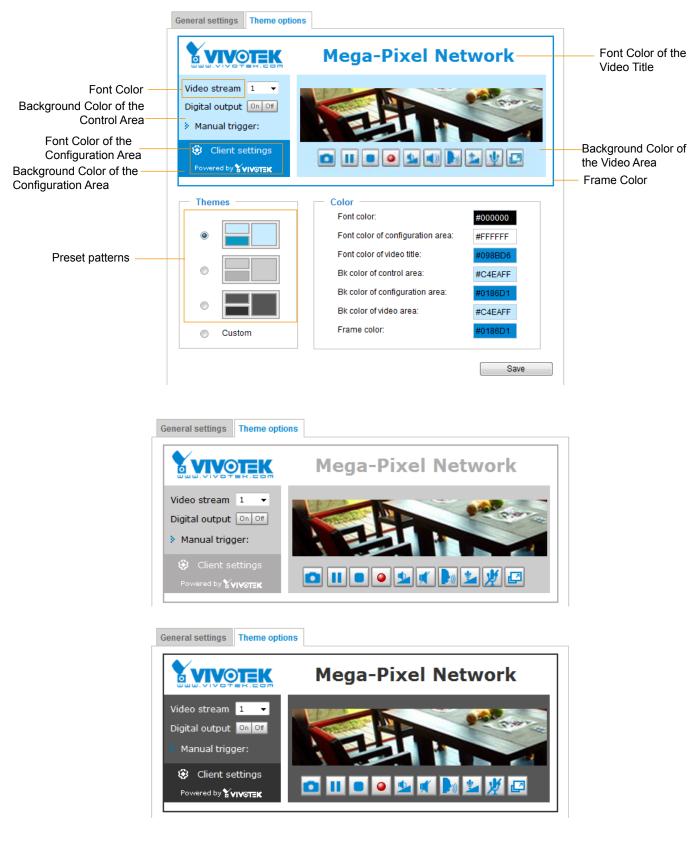
Customized button

If you want to hide manual trigger buttons on the homepage, please uncheck this item. This item is checked by default.

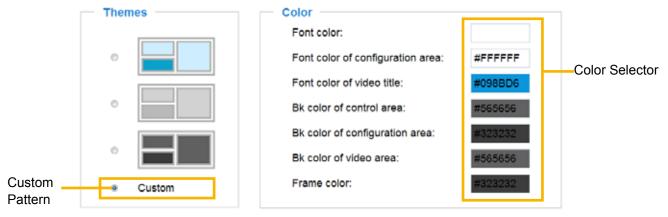
Customized button	
📝 Show manual trigger button	
	Save

Theme Options

Here you can change the color of your homepage layout. There are three types of preset patterns for you to choose from. The new layout will simultaneously appear in the **Preview** filed. Click **Save** to enable the settings.



- Follow the steps below to set up a custom homepage:
- 1. Click **Custom** on the left column.
- 2. Click to select a color on on the right column.



3. The palette window will pop up as shown below.

Hex:	#000000		02	Hex:	#23538A
Red:	0			Red:	35
Green:	0			Green:	83
Blue:	0			Blue:	138
Hue:	0			Hue:	212
Saturation:	0			Saturation:	74.6
Value:	0			Value:	54.1
Se	elect			4 Se	lect

- 4. Drag the slider bar and click on the left square to select a desired color.
- 5. The selected color will be displayed in the corresponding fields and in the **Preview** column.
- 6. Click **Save** to enable the settings.

System > Logs

This section explains how to configure the Network Camera to backup system log to a remote server.

Log server settings

Log server settings	
Enable remote log	
IP address:	
port:	514
	Save

Follow the steps below to set up the remote log:

- 1. Select Enable remote log.
- 2. In the IP address text box, enter the IP address of the remote server.
- 2. In the port text box, enter the port number of the remote server.
- 3. When completed, click **Save** to enable the setting.

You can configure the Network Camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the user install a log-recording tool to receive system log messages from the Network Camera. An example is Kiwi Syslog Daemon. Visit http://www.kiwisyslog. com/kiwi-syslog-daemon-overview/.

Cine Sector	(Serie)	wager Billing 1	ar - Veryner 9.2		Coll Column
File (181)	vier the	week main			
ê 3 m	山田 (Einglig (0.5Da	feeli +		Xi Days lef in work-store
()-de	Tee	Printy	Hardsoner	Herman	
06-27-2011	17.08.45	Spikightle	****.188.4 1023	springed 1.5.0 section	
06-27-2011	1258657	Dec.Mde	FSZ.168.4.103	DIRSP SERVER: Stop one access, IP-182 158 A121	
100-27-2011	17.06.57	El an Info	832.1084.103	hard annuance repeated 2 lines	
06-27-2811	17:06:13	User Jebs	882,168.4,103	(HTSP SERVER) Start and initials, IP-112 168.4.181	
100-27-2001	17-09-12	User Lover	100 168 4 103	(HSP HIMCH) and another programming and the Analytic SP Himself International Tele Analytics	Number of the statement of the State of The
06-27-2011	17:06:17	then left-	110 108 4 103	[UTSP 100MDI] XHLSP wave perk after discussed element of her 6"H	
06-27-2011	12:06:12	Unic. July	852,188.4.103	DUESP LEDIMENT: Shed one-assiston, IP-THE TAR 6.121	
06-27-2011	17.06.12	Uner July	832.168.4.103	[115P 109M08] Shoreeve annalas, #5-152 108 4 101	
06-27-2011	17.06.10	Uner Nielice	192.188.4.101	TUPHP DEVICE) Precess and	
06.27.2011	121608	Deer Nation	197-168-4.163	(1974 Envirol) Diating ODM stories.	
06-27-2011	12.06.07	they let	1121684103	[mastricking] finally to write high	
06-27-2011	17:56:05	Domain Notice	192,168.4.163	offrape: des 112,168,8.10.152,168,8.29	
100.70.36	17.06.06	Docum Nation	192 108 4 103	adapt: main 132.168.4.1	
06-37-2411	17:06:05	Distant Notice	112.108.4.103	offenet 1P 192,162,4,103 methods 275,255,255,0	
100.02.0001	110503	State Manufactor	100 100 4 100	CVENT MODE the assesses of event \$5 is chosen because of the priority ()	

System log

This column displays the system log in chronological order. The system log is stored in the Network Camera's buffer and dated events will be overwritten when the number of events reaches a limit.

System log	Access ing	
Jul 4 09:45	7 syslogd 1.5.0: restart	
Jul 4 09:45:4	e [swatchdog]: Ready to watch httpd.	11
Jul 4 09:45	9 (EVENT MGR). Starting eventing with support for EcTun	
Jul 4 09:45 4	9 (EVENT MGR); Task confile: there is no valid event in recording_task.xml, skip it	11
Jul 4 09:45	IS [EVENT MGR] Task confille: there is no valid event in event_task.xml, skip it	
Jul 4 09:45:5	1 [DRM Service] Starting DRM service.	
Jul 4 09.48.0	1 [UPnPIGDCP]. Search IGD failed	
Jul 4 09:46.0	1 [swatchdog]: Reduplicate registration from configer.	
Jul 4 99:46:0	1 [swatchdog]: Ready to watch configer.	
Jul 4 09:46:0	2 automount(723) >> mount: mounting /dev/mmcbik0p1 on /mnt/auto/CF failed: No	
such device	or address	
Jul 4 09:46:0	2 automount[723]; mount(generic); failed to mount /devimmcbik0p1 (type vfat)	
on /mnt/auto	CF	
Jul 4 09:46.0	2 automount[732]. >> mount: mounting /dev/mmcblk0p1 on /mnblauto/CF failed: No	
such device	or address	
Jul 4 09:46:0	2 automount(732); mount(generic); failed to mount /devimmcbik0p1 (type vfat)	
on /mnt/auto	ICF	
Jul 4 09:46:0	(2 [ThermalD]: Can not access thermal sensor!	
Jul 4 09:46:0	3 [SYS]: Serial number = 0002D112C715	
Jul 4 09.46.0	(3 (SY3): System starts at Mon Jul 4 09:46:03 UTC 2011	
Jul 4 09:46:0	3 (NET) === NET INFO ===	

Access log

Access log displays the access time and IP address of all viewers (including operators and administrators) in a chronological order. The access log is stored in the Network Camera's buffer and older events will be overwritten when the number of events reaches a limit.

System log Access log	
May 4 19:00:17 [RTSP SERVER]: Start one session, IP=192.168.4.101	*
May 4 19:00:39 [RTSP SERVER]: Stop one session, IP=192.168.4.101	
May 4 19:00:59 [RTSP SERVER]: Start one session, IP=192.168.4.101	
May 4 19:14:42 [RTSP SERVER]: Stop one session, IP=192.168.4.101	
May 4 19:16:11 [RTSP SERVER]: Start one session, IP=192.168.4.101	

System > Parameters

The View Parameters page lists the entire system's parameters in an alphabetical order. If you need technical assistance, use a text-editor program to copy and save the parameters listed on this page. Send the parameter text file to VIVOTEK's technical support.

```
Parameters
                                                                      .
                                                                      (E)
system hostname='Mega-Pixel Network Camera'
system ledoff='0'
system lowlight='1'
system_date='2013/12/12'
system_time='13:48:54'
system datetime=''
system_ntp=''
system_timezoneindex='320'
system daylight enable='0'
system_daylight_dstactualmode='1'
system daylight auto begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-160,
system updateinterval='0'
system info modelname='FE8174'
system_info_extendedmodelname='FE8174'
system_info_serialnumber='0002D126A90B'
system info firmwareversion='FE8174-VVTK-0100c'
system info language count='9'
system_info_language_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system info language i3='Français'
system_info_language_i4='Italiano
system_info_language_i5='日本語'
system info language i6='Português'
system info language i7='简体中文'
system info language i8='繁體中文'
system info language i9=''
4
                  111
```

System > Maintenance

This chapter explains how to restore the Network Camera to factory default, upgrade firmware version, etc.

General settings > Upgrade firmware

Upgrade firmware —		
Select firmware file:	Browse	Upgrade

This feature allows you to upgrade the firmware of your Network Camera. It takes a few minutes to complete the process.

Note: Do not power off the Network Camera during the upgrade!

Follow the steps below to upgrade the firmware:

- 1. Download the latest firmware file from the VIVOTEK website. The file is in .pkg file format.
- 2. Click **Browse...** and specify the firmware file.
- 3. Click **Upgrade**. The Network Camera starts to upgrade and will reboot automatically when the upgrade completes.

If the upgrade is successful, you will see "Reboot system now!! This connection will close". After that, reaccess the Network Camera.

The following message is displayed when the upgrade has succeeded.

Reboot system now!! This connection will close.

The following message is displayed when you have selected an incorrect firmware file.

Starting firmware upgrade Do not power down the server during the upgrade. The server will restart automatically after the upgrade is completed. This will take about 1 - 5 minutes. Wrong PKG file format Unpack fail
--

General settings > Reboot

Reboot	
(Reboot

This feature allows you to reboot the Network Camera, which takes about one minute to complete. When completed, the live video page will be displayed in your browser. The following message will be displayed during the reboot process.

The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/ If the connection fails, please manually enter the above IP address in your browser.

If the connection fails after rebooting, manually enter the IP address of the Network Camera in the address field to resume the connection.

General settings > Restore

_	Restore —			
	Restore all se	ettings to factory default exc	cept settings in	
	Network	Daylight saving time	🔲 Custom language 📄 VADP	Restore

This feature allows you to restore the Network Camera to factory default settings.

<u>Network</u>: Select this option to retain the Network Type settings (please refer to Network Type on page 69).

<u>Daylight Saving Time</u>: Select this option to retain the Daylight Saving Time settings (please refer to Import/Export files below on this page).

<u>Custom Language</u>: Select this option to retain the Custom Language settings.

<u>VADP</u>: Retain the VADP modules (3rd-party software stored on the SD card) and related settings.

If none of the options is selected, all settings will be restored to factory default. The following message is displayed during the restoring process.

The device is rebooting now. Your browser will reconnect to http://192.168.5.151:80/ If the connection fails, please manually enter the above IP address in your browser.	

Import/Export files

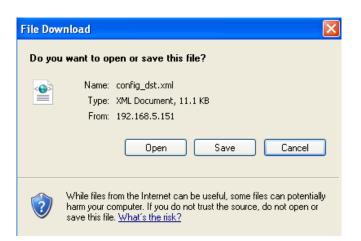
This feature allows you to Export / Update daylight saving time rules, custom language file, and configuration file.

Export files	
Export daylight saving time configuration file	Export
Export language file	Export
Export configuration file	Export
Export server status report	Export
Upload files	
Update daylight saving time rules:	Browse Upload
Update custom language file:	Browse Upload
Upload configuration file:	Browse Upload

Export daylight saving time configuration file: Click to set the start and end time of DST.

Follow the steps below to export:

- 1. In the Export files column, click **Export** to export the daylight saving time configuration file from the Network Camera.
- 2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.



3. Open the file with Microsoft[®] Notepad and locate your time zone; set the start and end time of DST. When completed, save the file.

In the example below, DST begins each year at 2:00 a.m. on the second Sunday in March and ends at 2:00 a.m. on the first Sunday in November.

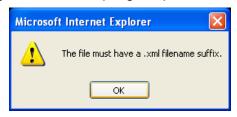
D co	nfig_dst - Notepad		
File E	dit Format View Help		
	<day><</day>	<pre><weekinmonth>First</weekinmonth> cbayofweek>sunday <dour>2</dour></pre>	
	<starttime <shift donth <day> <shift donth <day> </day></shift </day></shift </starttime 	>60 >3 >0ay> <weekinmonth>Second</weekinmonth> <dayofweek>Sunday</dayofweek> <hout>2</hout> >>60 >>11 //Day> <weekinmonth>First</weekinmonth> <dayofweek>Sunday</dayofweek> <hout>2</hout>	
	<timezone id="</td><td>-241" name="(GMT-06:00) Mexico City"></timezone>	×	
<			>

Update daylight saving time rules: Click Browse... and specify the XML file to update.

If incorrect date and time are assigned, you will see the following warning message when uploading the file to the Network Camera.



The following message is displayed when attempting to upload an incorrect file format.



<u>Export language file</u>: Click to export language strings. VIVOTEK provides nine languages: English, Deutsch, Español, Français, Italiano, 日本語, Português, 簡体中文, and 繁體中文.

<u>Update custom language file</u>: Click **Browse...** and specify your own custom language file to upload.

Export configuration file: Click to export all parameters for the device and user-defined scripts.

<u>Export daylight saving time configuration file</u>: Click **Browse...** to update a configuration file. Please note that the model and firmware version of the device should be the same as the configuration file. If you have set up a fixed IP or other special settings for your device, it is not suggested to update a configuration file.

Export server staus report: Click to export the current server status report, such as time, logs, parameters, process status, memory status, file system status, network status, kernel message..., and so on.



• If a firmware upgrade is accidentally disrupted, say, by a power outage, you still have a last resort method to restore normal operation. See the following for how to bring the camera back to work:

Applicable scenario:

- (1) Power disconnected during firmware upgrade.
- (2) Unknown reason causing abnormal LED status, and a Restore cannot recover normal working condition.

You can use the following methods to activate the camera with its backup firmware:

- (1) Press and hold down the reset button for at least one minute.
- (2) Power on the camera until the Red LED blinks rapidly.
- (3) After boot up, the firmware should return to the previous version before the camera hanged. (The procedure should take 5 to 10 minutes, longer than the normal boot-up process). When tthis process is completed, the LED status should return to normal.

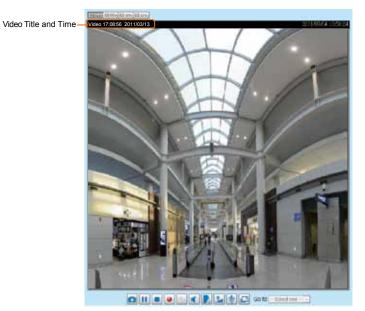
Media > Image

This section explains how to configure the image settings of the Network Camera. It is composed of the following tabbed windows: General settings, Image settings, Exposure, and Privacy mask, and Pixel Calculator.

General settings	General settings Image settings Exposure	Privacy mask Pixel calculator
	- Video Settings	
	Video title:	
	Show information in videos and snapshots	
	Mount type:	Ceiling Wall Floor
	Position of timestamp and video title on image:	Тор
	Timestamp and video title font-size:	Small 💌
	Color:	B/W O Color
	Power line frequency:	🔘 50 Hz 💿 60 Hz
	Video orientation:	Flip Mirror
	Day/Night settings	Save

<u>Video title</u>: Enter a name that will be displayed on the title bar of the live video as well as the view cell on the ST7501 and VAST recording software.

<u>Show information in videos and snapshots</u>: Enter a name that will be displayed on the title bar of the live video as the picture shown below.



Mount type: There are 3 Mount types - Ceiling, Wall, and Floor.

Ceiling: The Ceiling mount type automatically delivers upside-down images. The Ceiling mode supports the following Display modes - 10, 1P, 1R, 2P, 103R, 4R, 4R PRO, and 108R.

Wall: The Wall mount type applies to the monitoring of long, side-to-side surveillance areas, such as when mounted on a wall facing a corridor. Different Mount types have different options with the Display mode settings. For example, the **1P2R** (1 Panoramic & 2 Regional) and **1P3R** (1 Panoramic

& 3 Regional) Display modes are only available when the "Wall" Mount type is applied.

Floor: The Display modes with the Floor mount type are identical to those for the Ceiling mount except that the images are not vertically flipped.

<u>Position of timestamp and video title on image</u>: Select to display time stamp and video title on the top or at the bottom of the video stream.

<u>Timestamp and video title font size</u>: Select the font size for the time stamp and title.

<u>Color</u>: Select to display color or black/white video streams.

<u>Power line frequency</u>: Set the power line frequency consistent with local utility settings to eliminate image flickering associated with fluorescent lights.

<u>Video orientation</u>: Flip - vertically reflect the display of the live video; Mirror - horizontally reflect the display of the live video. Select both options if the Network Camera is installed upside-down (e.g., on the ceiling) to correct the image orientation. Please note that the preset locations will be cleared after you configure the flip/mirror option.

Day/Night Settings

This only provides a link to the Exposure window. See page 57 for details.

Image settings

On this page, you can tune the White balance, Image adjustment and WDR enhanced parameters. You can configure two sets of preferred settings: one for normal situations, the other for special situations, such as day/night/schedule mode.

	General settings image settings Counsels Privacy mank Pixel Calculator
	(Eises) (1.0%) (742-55) (742-55)
	White Judance Ada
Concer Cotting 1.	Dighness 0
Sensor Setting 1:	Coresset00
For normal situations	Saturation: 50%
	Sharphesis 50%
	Gamma colver Optimize 📼
	2 Enable low light compensation
	- WOR enhanced
Sensor Setting 2: For special	Enable MDR enhanced Profile Restore Save

F situations

White balance: Adjust the value for the best color temperature.

- Auto: It will automatically adjust the color temperature of the light in response to different light sources. You may follow the steps below to adjust the white balance to the best color temperature.
- 1. Set the White balance to Auto.
- 2. Place a sheet of white paper (or a color of a cool color temperature, such as blue) in front of the lens, then allow the Network Camera to adjust the color temperature automatically.
- 3. Check the **Off** button on **Fix current value** to confirm the setting when the camera automatically measured and adjusted the white balance.
- Manual: This item allows users to manually input the R gain & B gain ratios.

Image Adjustment

- Brightness: Adjust the image brightness level, which ranges from -5 to +5.
- Contrast: Adjust the image contrast level, which ranges from -5 to +5.
- Saturation: Adjust the image saturation level, which ranges from 0% to 100%. You can also select Customize and manually enter a value.

- Sharpness: Adjust the image sharpness level, which ranges from 0% to 100%.
- Gamma curve: Adjust the image sharpness level, which ranges from 0.45 to 1, from Detailed to Contrast. You may let firmware **Optimize** your display or select the **Manual** mode, and pull the slide bar pointer to change the preferred level of Gamma correction towards higher contrast or towards the higher luminance for detailed expression for both dark and lighted areas of an image.
- Enable low light compensation: Select this option in low light mode, and the values of sharpness and brightness will change automatically. This function also benefits from an automated noise reduction feature.

<u>Enable WDR enhanced</u>: This function allows users to identify more image details with an extreme contrast from an object of interest with one shadowed side against a bright background, e.g., an entrance. You may select the **Enable WDR enhanced** checkbox, and then adjust the strength (low, medium, high) to reach the best image quality.

WDR enhanced			
Enable WDR enhanced			
Strength:	Medium 💌		
Profile		Restore	Save

You can click on **Restore** to recall the original settings without incorporating the changes. When completed with the settings on this page, click **Save** to enable the setting.

If you want to configure another sensor setting for day/night/schedule mode, please click **Profile** to open the Profile Settings page as shown below.

Activated period Activated period Activated period Enable and apply this profile to Day mode Night mode Schedule mode White balance Auto Fix current value: On Off Image adjustment Brightness 5 Contrast 0 Subration: 50% Sharpness. 50% Gamma curve: Optimize Stharpness. 50% Gamma curve: Optimize Enable low light compensation WDR enhanced		Fichere (TCP-V)		
White balance Auto Fix current value: On Image adjustment Brightness -5 Brightness -5 O Saturation: 50% 50% Gamma curve: Optimize 90% Image adjust compensation WDR enhanced VDR enhanced	Auto Fix current value: On Off Image adjustment Image adjustment 5 Brightness: - - 5 Contrast 0 0 50% Sharpness: - 50% 50% Gamma curve: Ootimize 50% IV Enable low light compensation WDR enhanced - Image adjustment - - - Image adjustment - - - Image adjustment - - - - Sharpness: - - - - - Staturation: - - - - - - Staturation: -	Day mode	y this profile to	
Auto Fix current value: On Off Image adjustment -5 -5 Brightness -5 0 Saturation: 50% 50% Sharpness. 0 50% Gamma curve: Optimize 50% Image adjustment VDR enhanced VDR enhanced	Auto Fix current value: On Off Image adjustment Image adjustment -5 Brightness:		te	
Brightness -5 Contrast 0 Saturation: 50% Sharpness 50% Gamma curve: Optimize • [2] Enable low light compensation WDR enhanced	Brightness: -5 Contrast 0 Saturation: 50% Sharpness: 0 Gamma curve: Optimize • [V] Enable low light compensation WDR enhanced [II] Enable WDR enhanced III		Fix current value: On Off	
Contrast 0 Saturation: 50% Sharpness. 50% Gamma.curve: Optimize [V] Enable low light compensation WDR enhanced	Contrast 0 Saturation: 50% Sharpness. 50% Gamma curve: Optimize P Enable low light compensation WDR enhanced Enable WDR enhanced	Image adjustment	i	
Saturation: 50% Sharpness. 50% Gamma curve: Optimize • [9] Enable low light compensation WDR enhanced	Saturation: 50% Sharpness. 50% Gamma curve: Optimize V Enable low light compensation WDR enhanced Enable WDR enhanced	Brightness.	0	5
Sharpness. 50% Gamma curve: Optimize [2] Enable low light compensation WDR enhanced	Sharpness. 50% Gamma curve: Optimize	Contrast	O	٥
Gamma curve: Optimize 💽 [9] Enable low light compensation WDR enhanced	Gamma curve: Optimize	Saturation	O	50%
Enable low light compensation WDR enhanced	Enable low light compensation WDR enhanced Enable WDR enhanced	Sharpness.		
Enable low light compensation WDR enhanced	Enable low light compensation WDR enhanced Enable WDR enhanced		Optimize -	
WDR enhanced	WDR enhanced			
	Enable WDR enhanced			
			annad	

Please follow the steps below to setup a profile:

- 1. Select the Enable and apply this profile checkbox.
- Select the applied mode: Day mode, Night mode, or Schedule mode. Please manually enter a range of time if you choose Schedule mode.
- 3. Configure the White balance and Image adjustment settings in the following columns. Please refer to the previous page for detailed information.
- 4. Click **Save** to enable the settings and click **Close** to exit the page.

Exposure

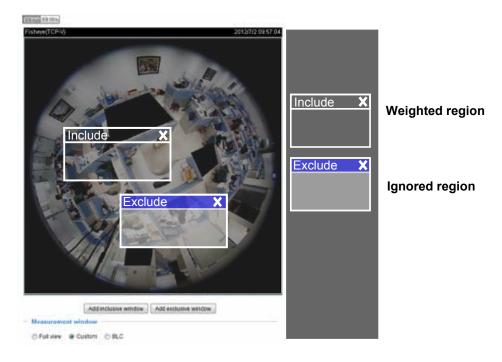
On this page, you can set the Exposure measurement window, Exposure level, Exposure mode, Exposure time, Gain control, and Day/Night mode settings. You can configure two sets of Exposure settings: one for normal situations, the other for special situations, such as the day/night/schedule mode.

	General settings Image settings Exposure Privacy mask Pixel calculator
	PERM DAMA
	(TCEAU) 2013/11/22 10.12.24 (TCEAU) (TCEAU) (TCEAU) (TCEAU) (TCEAU) (TCEAU) (TCEAU) (TCEAU) (TCEAU) (TCEAU) (TCEAU) (TCEAU)
Sensor Setting 1:	Exposure control
	Exposure time: 0 1/32000 - 1/30 Gain control: 0 - 100 %
Sensor Setting 2: For special situations	Profisi Restore Save

<u>Measurement Window</u>: This function allows users to set measurement window(s) for low light compensation. For example, where low-light objects are posed against an extremely bright background. You may want to exclude the bright sunlight shining through a building's corridor.

- Full view: Calculate the full range of view and offer appropriate light compensation.
- Custom: This option allows you to manually add customized windows as inclusive or exclusive regions. A total of 10 windows can be configured. Please refer to the next page for detailed illustration.

The inclusive window refers to the "weighted window"; the exclusive window refers to "ignored window". It adopts the weighted averages method to calculate the value. The inclusive windows have a higher priority. You can overlap these windows, and, if you place an exclusive window within a larger inclusive window, the exclusive part of the overlapped windows will be deducted from the inclusive window. An exposure value will then be calculated out of the remaining of the inclusive window.



BLC (Back Light Compensation): This option will automatically add a "weighted region" in the middle of the window and give the necessary light compensation.

Exposure control:

- Exposure level: You can manually set the Exposure level, which ranges from -2.0 to +2.0 (dark to bright).
- Flickerless: Under some circumstances when there is a difference between the video capture frequency and local AC power frequency (NTSC or PAL), the mismatch causes color shifts or flickering images. If the above mismatch occurs, select the Flickerless checkbox, and the range of Exposure time (the shutter time) will be limited to a range in order to match the AC power frequency. See the screen capture below.

You can click and drag the semi-circular pointers on the **Exposure time** and **Gain control** slide bars to specify a range of shutter time and Gain control values within which the camera can automatically tune to an optimal imaging result. For example, you may prefer a shorter shutter time to better capture moving objects, while a faster shutter reduces light and needs to be compensated by electrical brightness gains.



ay/Night		
<u> </u>	- Day/Night	
	Switch to B/W in	night mode
	Turn on external	IR illuminator in night mode
	IR cut filter:	Auto mode
	Sensitivity:	Normal
	Select auto mode v	vill disable profile of exposure settings.

Switch to B/W in night mode

Select this checkbox to enable the Network Camera to automatically switch to Black & White display during the night mode.

Turn on external IR illuminator in night mode

If your camera is installed with an IR illuminator and the digital output signals are connected to it, you can let system firmware turn on the supplementary illuminator during low-light conditions.

IR cut filter

With a removable IR-cut filter, this Network Camera can automatically remove the filter to let Infrared light pass into the sensor during low light conditions.

- Auto mode (The Day/Night Exposure Profile will not be available if Auto mode is selected) The Network Camera automatically removes the filter by judging the level of ambient light.
- Day mode

In day mode, the Network Camera switches on the IR cut filter at all times to block infrared light from reaching the sensor so that the colors will not be distorted.

Night mode

In night mode, the Network Camera switches off the IR cut filter at all times for the sensor to accept infrared light, thus helping to improve low light sensitivity.

Synchronize with digital input

The Network Camera automatically removes the IR cut filter when a digital input is triggered, for example, when the camera is accompanied by an external IR light that comes with its own sensor and provides a signal to the camera. Some camera housings come with such mechanism.

Schedule mode

The Network Camera switches between day mode and night mode based on a specified schedule. Enter the start and end time for day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the start and end time of a day mode are set to 07:00 and 18:00.

<u>Sensitivity</u>

Tune the responsiveness of the IR filter to lighting conditions as Low, Normal, or High.

When completed with the settings on this page, click **Save** to enable the settings.

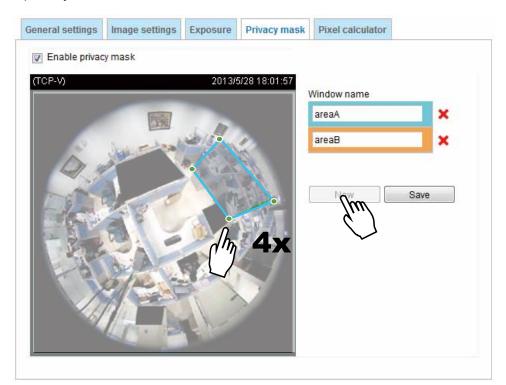
If you want to configure another sensor setting for a specific lighting condition in day/night/schedule mode, please click **Profile** to open the Profile settings page as shown below.

Please follow the steps below to setup a profile:

- 1. Check Enable and apply this profile.
- 2. Select the applied mode: **Day mode**, **Night mode**, or **Schedule mode**. Please manually enter a range of time through which you want the Schedule mode to apply.
- 3. Configure Exposure control settings in the following columns. Please refer to the previous page for detailed information.
- 4. Click **Save** to enable the setting and click **Close** to exit the window.

Privacy mask

Click **Privacy Mask** to open the settings page. On this page, you can block out certain sensitive zones to address privacy concerns.



- To set the privacy mask windows, follow the steps below:
- 1. Click New to add a new window. A text box will appear allowing you to enter a name for the mask.
- 2. Use four mouse clicks to mark a square area, which is recommended to be at least twice the size of the object (height and width) you want to cover.
- 3. Enter a Window Name and click **Save** to enable the setting.
- 4. Check Enable privacy mask to enable this function.

NOTE:

- ▶ Up to 5 privacy mask windows can be configured on the same screen.
- ► To delete a mask, use the red cross button and then click on the **Save** button.

Pixel Calculator

Pixel Calculator Window1 (H)x(V)

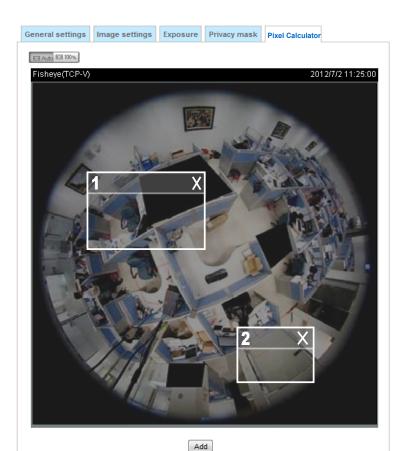
Stream1: 551x373

Stream2: 55x37

Stream3: 551x373

Click the **Add** button at the lower screen to create a pixel calculator window. Place your cursor on the window to move it to an area of your interest, and change the size of window to fit the area of interest.

Once they are drawn, the numbers of pixels on the sides of windows will appear. This allows you to calculate if your current configuration fulfills a requirement, for instance, for recognizing the faces of persons passing through a location. A facial recognition usually requires around 130 pixels per meter or higher.



Window2 (H)x(V)

Stream1: 555x370

Stream2: 55x37

Stream3: 555x370

The pixels thus calculated are listed at the lower screen on a per-stream basis depending on the frame size you configure for each video stream.

Media > Video

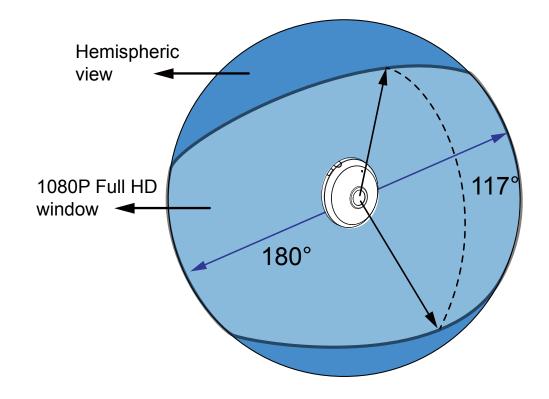
FOV

The Field of View window allows you to select either the Fisheye mode or a 1080P Full HD mode. The 1080P Full HD mode provides a dewarpped section (1920x1080 pixels) out of the 180 degrees hemispheric view. The 1080P Full HD mode provides a higher frame rate of up to 30fps. It is as if using the fisheye camera as a standard fixed dome camera with a wide view angle.

In the 1080P Full HD mode, regional and panoramic view modes will not be available. Also, changing the FOV option will erase the motion detection, privacy mask, and preset postions you previously configured.

FOV Stream	m
F	isheye mode (MAX 15fps)
© 1	080P Full HD (MAX 30fps)

Below is a conceptual drawing showing the coverage of the 1080P Full HD mode.



🖉 NOTE:

If the FOV 1080P mode is selected, the Local dewarp function will not be available.

Media > Video

Stream settings

FOV	
Video settings for stream 1	
Video settings for stream 2	
Video settings for stream 3	
	Save

This Network Camera supports multiple streams with frame size ranging from 192 x 192 to 1920 x 1920.

Please follow the steps below to set up those settings for an individual stream:

- 1. Select a stream to configure its viewing region.
- 2. Choose a proper **Frame Size** from the drop-down list according to the size of monitored device.
- 3. Select the Maximum frame rate.
- The parameters of the multiple streams:

	Frame size	
Stream 1	1920 x 1920 ~ 192 x 192 (Selectable)	
Stream 2	1920 x 1920 ~ 192 x 192 (Selectable)	
Stream 3	1920 x 1920 ~ 192 x 192 (Selectable)	

To change the frame size, frame rate, and other related settings, click on video settings for a video stream to its individual configuration panel.

Video settings for stream 1		Video settings for stream 3	
Local dewarp mode	10 💌	MPEG-4	
© MPEG-4		-	
# H.264		H.264	
Frame size:	1920x1920 -	Frame size:	1920x1920 💌
Maximum frame rate:	15 fps 💌	Maximum frame rate:	15 fps 💌
intra frame period.	15 .	Intra frame period:	1 S 💌
Video quality		Video quality	
Constant bit rate:		Constant bit rate:	
Target bit rate	4Mbps 💌	<u> </u>	
Policy:	Frame rate priority	Fixed quality:	
C Fixed quality:		Quality:	Good 👻
() JPEG		Maximum bit rate:	40 Mbps 👻
Video settings for stream 2		◎ JPEG	
Local dewarp mode	10 -		
O MPEG-4			
# H 264			
Frame size:	512x512 .		
Maximum frame rate:	S fps 🗶		
Intra frame period.	15 .		
Video quality			
· Constant bit rate			
Target bit rate	40Kbps 💌		
Policy:	Frame rate priority		
Fixed quality:			
© JPEG			

Click the stream item to display the detailed information.

This Network Camera offers real-time H.264, MPEG-4 and MJPEG compression standards (Triple Codec) for real-time viewing.

If H.264 or MPEG-4 mode is selected, the video is streamed via RTSP protocol. There are several parameters for you to adjust the video performance:

MPEG-4		
H.264		
Frame size	E.	512x512 💌
Maximum f	rame rate:	5 fps 💌
Intra frame	period:	1 S 💌
Video qual	ity	
O Co	nstant bit rate:	
1	Farget bit rate:	40Kbps 💌
ŧ	Policy:	Frame rate priority
) Fix	ed quality:	
IPEG		

■ Local dewarp mode

Mount type	Configurable Display Modes	
Ceiling / Floor	10, 1P, 2P, 1R, 4R	
Wall	10, 1P, 1R, 4R	

Local dewarp is designed for 3rd-party software that has not implemented the dewarp plug-ins. Plugins are required to convert a fisheye image into a regional or panoramic view. Without the plug-ins, you can only see the original circular view on a client computer. If configured, the dewarp process takes place on the network camera, rather than on the client computer. The camera then delivers the dewarped view of video stream to the client side.

Fisheye functions	Client-side dewarp	Local dewarp
Pan/tilt on Regional view	Yes	N/A, fixed view
Pan on Panoramic view	Yes	N/A, fixed view
Zoom in/out on Regional view	Yes	N/A
Change of Display mode	10	Fixed, configured in firmware console: Media > Video
Available Display modes	10, 1P, 1R, 2P, 103R, 4R, 4R Pro, 108R, 1P2R, 1P3R	10, 1P, 2P, 1R, 4R

Note that once the video has been dewarped on the camera side, you will not be able to utilize the zoom in, zoom out, and PTZ control on the client computer. And, for example, you can not change the view angle of a regional view on the live view page. The view angle is configured on the PTZ > PTZ settings window. Please refer to page 96 for more information.

Also note the following when using the Local dewarp:

- To disable the Local dewarp function, select the **10** mode from its pull-down menu.
- Local dewarp is configurable on stream #1 and stream #2.
- The PTZ control panel on the main page is not available with the video stream on which the Local dewarp is applied.
- Each video stream can be configured with an individual local dewarp mode.
- If you change the mount type settings, the Local dewarp configuration will be erased. The camera then resumes the original 10 display mode.
- The PTZ preset positions have been cancelled in this revision of firmware.
- Note that some software vendors, such as Milestone®, has already implemented the support for VIVOTEK's plug-ins. You only need to download and install plug-ins for use with Milestone's software.

Frame size

You can set up different video resolutions for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoothlier video quality.

Regardless of the power line frequency setting (60Hz or 50Hz), the frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, 12fps, and 15fps. You can also select **Customize** and manually enter a value.

Intra frame period

Determine how often to plant an I frame. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds, and 4 seconds.

- Video quality
 - <u>Constant bit rate</u>: A complex scene generally produces a larger file size, meaning that higher bandwidth will be needed for data transmission. The bandwidth utilization is configurable to match a selected level, resulting in mutable video quality performance. The bit rates are selectable at the following rates: 20Kbps, 30Kbps, 40Kbps, 50Kbps, 64Kbps, 128Kbps, 256Kbps, 512Kbps, 768Kbps, 1Mbps, 2Mbps, 3Mbps, 4Mbps, 6Mbps, 8Mbps, and 16Mbps. You can also select **Customize** and manually enter a value up to 40Mbps.

- Target bit rate: select a bit rate from the pull-down menu. The bit rate ranges from 20kbps to a maximum of 16Mbps. The bit rate then becomes the Average or Upper bound bit rate number. The Network Camera will strive to deliver video streams around or within the bit rate limitation you impose.

- Policy: If Frame Rate Priority is selected, the Network Camera will try to maintain the frame rate per second performance, while the image quality will sometimes be compromised. If Image quality priority is selected, the Network Camera might drop some video frames in order to maintain image quality.

• <u>Fixed quality</u>: On the other hand, if **Fixed quality** is selected, all frames are transmitted with the same quality; bandwidth utilization is therefore unpredictable. The video quality can be adjusted to the following settings: Medium, Standard, Good, Detailed, and Excellent. You can also select **Customize** and manually enter a value.

- Maximum bit rate: With the guaranteed image quality, you might still want to place a bit rate limitation to control the size of video streams for bandwidth and storage concerns. The configurable bit rate starts from 1Mbps to 40Mbps.

The Maximum bit rate setting in the Fixed quality configuration can ensure a reasonable and limited use of network bandwidth. For example, in low light conditions where a Fixed quality setting is applied, video packet sizes can tremendously increase when noises are produced with electrical gain.

You may also manually enter a bit rate number by selecting the **Customized** option.

If **JPEG** mode is selected, the Network Camera continuously sends JPEG images to the client, producing a moving effect similar to a filmstrip. Every single JPEG image transmitted guarantees the same image quality, which in turn comes at the expense of variable bandwidth usage. Because the media contents are a combination of JPEG images, no audio data is transmitted to the client. There are three parameters provided in MJPEG mode to control the video performance:

IPEG			
Fran	ne size:	1920x1920	•
Maxi	mum frame rate:	15 fps	-
Vide	o quality	Good	-

Frame size

You can set up different video resolution for different viewing devices. For example, set a smaller frame size and lower bit rate for remote viewing on mobile phones and a larger video size and a higher bit rate for live viewing on web browsers. Note that a larger frame size takes up more bandwidth.

Maximum frame rate

This limits the maximum refresh frame rate per second. Set the frame rate higher for smoother video quality.

The frame rates are selectable at 1fps, 2fps, 3fps, 5fps, 8fps, 10fps, and 15fps. You can also select **Customize** and manually enter a value. The frame rate will decrease if you select a higher resolution.

Video quality

Refer to the previous page setting an average or upper bound threshold for controlling the bandwidth consumed for transmitting motion jpegs. The configuration method is identical to that for MPEG4 and H.264.



- Video quality and fixed quality refers to the compression rate. If you select to enter a Customized value in the Fixed quality menu, a lower value will produce higher quality.
- Converting high-quality video may significantly increase the CPU loading, and you may encounter streaming disconnection or video loss while capturing a complicated scene. In the event of occurance, we suggest you customize a lower video resolution or reduce the frame rate to obtain smooth video.

Media > Audio

Audio Settings

Mute				
Microphone source:	Internal 💌			
Internal microphone input gain:				69%
External microphone input gain:	0	-0-	100%	69%
Audio type	0		100%	
AAC bit rate:	16 Kbps 💌			
© G.711:	pcmu 💌			
G.726 bit rate:	32 Kbps 💌			

<u>Mute</u>: Select this option to disable audio transmission from the Network Camera to all clients. Note that if mute mode is turned on, no audio data will be transmitted even if audio transmission is enabled on the Client Settings page. In that case, the following message is displayed:

Warning
The media type has been changed to video only because the media from server contains no audio
ОК

Internal microphone input gain: Select the gain of the internal audio input according to ambient conditions. Adjust the gain from -33dB (least) to 21dB (most).

External microphone input gain: Select the gain of the external audio input according to ambient conditions. Adjust the gain from -33dB (least) to 21dB (most).

Audio type: Select audio codec AAC, GSM-AMR, or G.711 and the bit rate.

- AAC provides good sound quality at the cost of higher bandwidth consumption. The bit rates are selectable from: 16Kbps, 32Kbps, 48Kbps, 64Kbps, 96Kbps, and 128Kbps.
- G.711 also provides good sound quality and requires about 64Kbps. Select pcmu (µ-Law) or pcma (A-Law) mode.
- G.726 is a speech codec standard covering voice transmission at rates of 16, 24, 32, and 40kbit/s.

When completed with the settings on this page, click **Save** to enable the settings.

Network > General settings

This section explains how to configure a wired network connection for the Network Camera.

 LAN Get IP address automatically Use fixed IP address Enable UPnP presentation Enable UPnP port forwarding PPPoE Enable IPv6 	Network Type	Network type
 Use fixed IP address Enable UPnP presentation Enable UPnP port forwarding PPPoE 		LAN LAN
 Enable UPnP presentation Enable UPnP port forwarding PPPoE 		 Get IP address automatically
 Enable UPnP port forwarding PPPoE 		Use fixed IP address
© PPPoE		Enable UPnP presentation
		Enable UPnP port forwarding
Enable IPv6		O PPPoE
		Enable IPv6
Save		

LAN

Select this option when the Network Camera is deployed on a local area network (LAN) and is intended to be accessed by local computers. The default setting for the Network Type is LAN. Rememer to click **Save** when you complete the Network setting.

<u>Get IP address automatically</u>: Select this option to obtain an available dynamic IP address assigned by the DHCP server each time the camera is connected to the LAN.

Use fixed IP address: Select this option to manually assign a static IP address to the Network Camera.

Network type			
AN			
Get IP address automatically			
Use fixed IP address			
IP address:	192.168.4.108		
Subnet mask:	255.255.255.0		
Default router:	192.168.4.1		
Primary DNS:	192.168.0.10		
Secondary DNS:	192.168.0.20		
Primary WINS server:	192.168.0.10		
Secondary WINS server:	192.168.0.20		
Enable UPnP presentation			
Enable UPnP port forwarding			
O PPPoE			
Enable IPv6			
		99	ve

- 1. You can make use of VIVOTEK Installation Wizard 2 on the software CD to easily set up the Network Camera on LAN. Please refer to Software Installation on page 19 for details.
- 2. Enter the Static IP, Subnet mask, Default router, and Primary DNS provided by your ISP.

<u>Subnet mask</u>: This is used to determine if the destination is in the same subnet. The default value is "255.255.255.0".

<u>Default router</u>: This is the gateway used to forward frames to destinations in a different subnet. Invalid router setting will fail the transmission to destinations in different subnet.

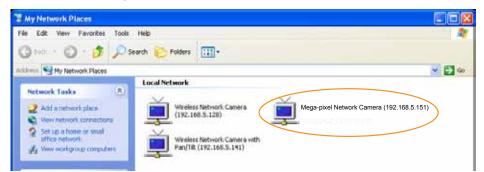
Primary DNS: The primary domain name server that translates hostnames into IP addresses.

<u>Secondary DNS</u>: Secondary domain name server that backups the Primary DNS.

<u>Primary WINS server</u>: The primary WINS server that maintains the database of computer name and IP address.

<u>Secondary WINS server</u>: The secondary WINS server that maintains the database of computer name and IP address.

<u>Enable UPnP presentation</u>: Select this option to enable UPnP[™] presentation for your Network Camera so that whenever a Network Camera is presented to the LAN, shortcuts of connected Network Cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP[™] is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP[™] component is installed on your computer.



<u>Enable UPnP port forwarding</u>: To access the Network Camera from the Internet, select this option to allow the Network Camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize of this feature, make sure that your router supports UPnPTM and it is activated.

PPPoE (Point-to-point over Ethernet)

Select this option to configure your Network Camera to make it accessible from anywhere as long as there is an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire your Network Camera's public IP address.

- 1. Set up the Network Camera on the LAN.
- 2. Go to Configuration > Event > Event settings > Add server (please refer to Add server on page 107) to add a new email or FTP server.
- 3. Go to Configuration > Event > Event settings > Add media (please refer to Add media on page 111). Select System log so that you will receive the system log in TXT file format which contains the Network Camera's public IP address in your email or on the FTP server.
- 4. Go to Configuration > Network > General settings > Network type. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.

© LAN	
PPPoE	
User name:	
Password:	
Confirm password:	
Enable IPv6	
	Save

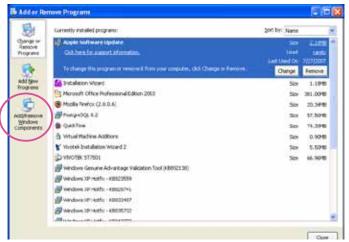
- 5. The Network Camera will reboot.
- 6. Disconnect the power to the Network Camera; remove it from the LAN environment.

NOTE:

- ► If the default ports are already used by other devices connected to the same router, the Network Camera will select other ports for the Network Camera.
- If UPnP[™] is not supported by your router, you will see the following message: Error: Router does not support UPnP port forwarding.
- ► Below are steps to enable the UPnPTM user interface on your computer: Note that you must log on to the computer as a system administrator to install the UPnPTM components.
 - 1. Go to Start, click Control Panel, then click Add or Remove Programs.

Anna Charles Ind	and an and a second second	
O constan		×.0-
D restations for	Pick a category	
Bartha D	And a second second second	Contraction and the second
Contractions Contractions	🚽 na start berret beserve	- 🥂
* hank of tool	(in	and the local sector of here of the sector o
		- d
	-	
	The set of the second	

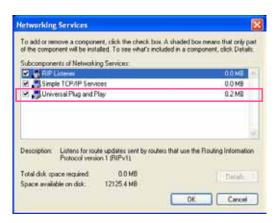
2. In the Add or Remove Programs dialog box, click Add/Remove Windows Components.



3. In the Windows Components Wizard dialog box, select Networking Services and click Details.

indows Components You can add or remove components of	Windows XP	
	e checkbox. A shaded box means that o To see what's included in a component, o	
C Message Queuing	0.0 MB	
M WINE close	135.60	1
www.Newniting.Services	03148	
Cher Network File and First Se	Nices 0.0 MB	1
the second state of the state of the	TIÓ ME	
Contraction Boot Certificates		
	alized, retwort selated services and proto	con
Desception Contains a variety of speci	0 MB	colt

4. In the Networking Services dialog box, select Universal Plug and Play and click OK.



5. Click Next in the following window.

ndows Components You can add or remove components of Windows 30 ⁹	
To add to remove a component, click the checkbox, part of the component will be installed. To see what's	
Details	exercise of a completent, once
Components:	
Set Message Queung	0.0 MB
🔀 📌 MSN Explorer	13.5 MB
P to Networking Learning	0.2 MB
C Other Network File and Part Services	0.0 MB
Fall Indete Boot Cetificates	nome 🛎
Description: Contains a variety of specialized, network	ik selated services and protocols
Total dels space required 0.0 MB	C. Park
	Details.

- 6. Click **Finish**. UPn P^{TM} is enabled.
- ► How does $UPnP^{TM}$ work?

UPnP[™] networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available among each other without the need for cumbersome network configuration. In the case of Network Cameras, you will see Network Camera shortcuts under My Network Places.

Enabling UPnP port forwarding allows the Network Camera to open a secondary HTTP port on the router-not HTTP port-meaning that you have to add the secondary HTTP port number to the Network Camera's public address in order to access the Network Camera from the Internet. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

From the Internet	In LAN
http://203.67.124.123:8080	http://192.168.4.160 or http://192.168.4.160:8080

If the PPPoE settings are incorrectly configured or the Internet access is not working, restore the Network Camera to factory default; please refer to **Restore** on page 49 for details. After the Network Camera is reset to factory default, it will be accessible on the LAN.

Enable IPv6

Select this option and click Save to enable IPv6 settings.

Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft[®] Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

Network type		
© LAN		
PPPoE		
User name:]	
Password:]	
Confirm password:]	
Enable IPv6		
IPv6 information		
Manually setup the IP address		
		Save

When IPv6 is enabled, by default, the network camera will listen to router advertisements and be assigned with a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information as shown below.

	<u>close</u>
[eth0 address] fe80:0000:0000:0000:0202:d1ff:fe0e:d4c8/64@Link [Gateway]]
IPv6 address list of gateway	
[DNS]	_
IPv6 address list of DNS	
- 1111 J WIL 144J	

If your IPv6 settings are successful, the IPv6 address list will be listed in the pop-up window. The IPv6 address will be displayed as follows:

Refers to Ethernet

Link-global IPv6 address/network mask
Link-local IPv6 address/network mask
-

Please follow the steps below to link to an IPv6 address:

- 1. Open your web browser.
- 2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
- 3. The format should be:



4. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage. For example:

Network Camera - Microsoft Internet Explorer File Edit View Favorites Tools Help	
G Back ▼ O Image: Second sec	🖉 - 🍃 🗃 🖓
Address http://[2001:0c08:2500:0002:0202:d1ff:fe04:65f4]/	
VIVOTEK	

NOTE:

If you have a Secondary HTTP port (the default value is 8080), you can also link to the webpage in the following address format: (Please refer to HTTP streaming on page 77 for detailed information.)



► If you choose PPPoE as the Network Type, the [PPP0 address] will be displayed in the IPv6 information column as shown below.

[eth0 address] fe80.0000.0000.0000.0202.d1ff:fe11.2299/64@Link
[ppp0 address] fe80.0000.0000.0000.0202.d1ff:fe11:2299/10@Link
2001:b100:01c0:0002:0202:d1ff:fe11:2299/64@Global
[Gateway]
fe80::90:1a00:4142:8ced
[DNS]
2001:6000::1

<u>Manually setup the IP address</u>: Select this option to manually set up IPv6 settings if your network environment does not have DHCPv6 server and router advertisements-enabled routers. If you check this item, the following blanks will be displayed for you to enter the corresponding information:

64

Port

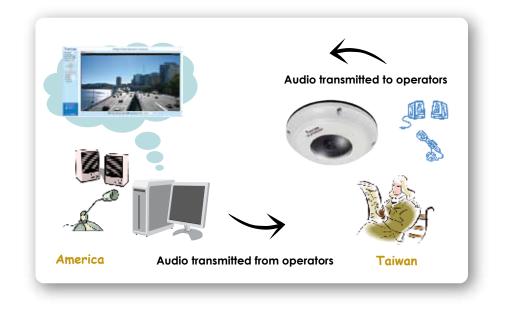
port	
HTTPS port:	443
Two way audio port:	5060
FTP port:	21

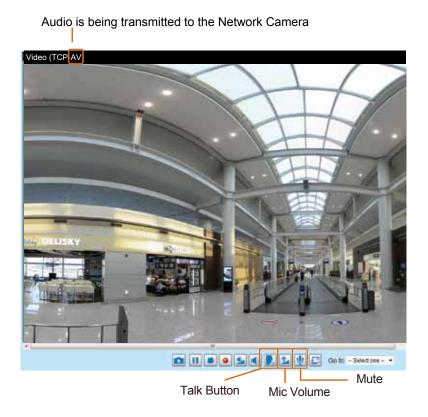
<u>HTTPS port</u>: By default, the HTTPS port is set to 443. It can also be assigned to another port number between 1025 and 65535.

<u>Two way audio port</u>: By default, the two way audio port is set to 5060. Also, it can also be assigned to another port number between 1025 and 65535.

The Network Camera supports two way audio communication so that operators can transmit and receive audio simultaneously. By using the Network Camera's built-in or external microphone and an external speaker, you can communicate with people around the Network Camera.

Note that as JPEG only transmits a series of JPEG images to the client, to enable the two-way audio function, make sure the video mode is set to "MPEG-4" or "H.264" on the Media > Video > Stream settings page and the media option is set to "Media > Video > Stream settings" on the Client Settings page. Please refer to Client Settings on page 39 and Stream settings on page 63.





Click **r** to enable audio transmission to the Network Camera; click **r** to adjust the volume of microphone; click **v** to turn off the audio. To stop talking, click **r** again.

<u>FTP port</u>: The FTP server allows the user to save recorded video clips. You can utilize VIVOTEK's Installation Wizard 2 to upgrade the firmware via FTP server. By default, the FTP port is set to 21, or assigned to another port number between 1025 and 65535.

Network > Streaming protocols

HTTP streaming

To utilize HTTP authentication, make sure that your have set a password for the Network Camera first; please refer to Security > User account on page 88 for details.

HTTP streaming	RTSP streaming		
Authentication:		basic 👻	
HTTP port:		80	
Secondary HTTP po	ort:	8080	
Access name for s	tream 1:	video.mjpg	
Access name for s	tream 2:	video2.mjpg	
Access name for s	tream 3:	video3.mjpg	
			Save

<u>Authentication</u>: Depending on your network security requirements, the Network Camera provides two types of security settings for an HTTP transaction: basic and digest.

If **basic** authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

<u>HTTP port / Secondary HTTP port</u>: By default, the HTTP port is set to **80** and the secondary HTTP port is set to **8080**. They can also be assigned to another port number between 1025 and 65535. If the ports are incorrectly assigned, the following warning messages will be displayed:



To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080, refer to the list below for the Network Camera's IP address.

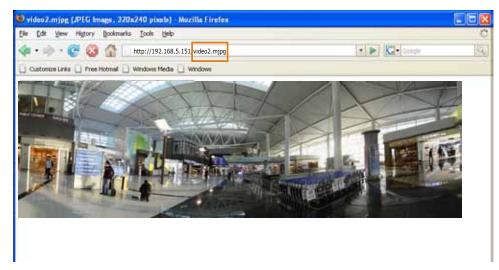
On the LAN
http://192.168.4.160 or
http://192.168.4.160:8080

<u>Access name for stream 1 ~ 3</u>: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Media > Video > Stream settings** to set up the video quality of linked streams. For more information about how to set up the video quality, please refer to Stream settings on page 63.

When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to **JPEG**, users will receive video comprised of continuous JPEG images. This technology, known as "server push", allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape.

URL command -- http://<ip address>:<http port>/<access name for stream 1 ~ 5> For example, when the Access name for stream 2 is set to video2.mjpg:

- 1. Launch Mozilla Firefox or Netscape.
- 2. Type the above URL command in the address bar. Press Enter.
- 3. The JPEG images will be displayed in your web browser.



M IMPORTANT:

- Microsoft[®] Internet Explorer does not support server push technology; therefore, using http://<ip address>:<http port>/<access name for stream 1 ~ 3> will fail to access the Network Camera.
- Users can only use URL commands to request the stream 5. For more information about URL commands, please refer to page 135.

RTSP Streaming

To utilize RTSP streaming authentication, make sure that you have set a password for the Network Camera first; please refer to **Security > User account** on page 88 for details.

HTTP streaming	RTSP streaming		
Authentication:		disable	-
Access name for st	tream 1:	live.sdp	
Access name for st	tream 2:	live2.sdp)
Access name for st	tream 3:	live3.sdp)
RTSP port:		554	
RTP port for video:		5556	
RTCP port for video	:	5557	
RTP port for audio:		5558	
RTCP port for audio:		5559	

<u>Authentication</u>: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest.

If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If **digest** authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.

The availability of the RTSP streaming for the three authentication modes is listed in the following table:

	Quick Time player	VLC Player
Disable	0	0
Basic	0	0
Digest	0	Х

<u>Access name for stream 1 \sim 3</u>: This Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source.

If you want to use an RTSP player to access the Network Camera, you **HAVE TO** set the video mode to H.264 / MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.

rtsp://<ip address>:<rtsp port>/<access name for stream1 ~ 3>

For example, when the access name for stream 1 is set to live.sdp:

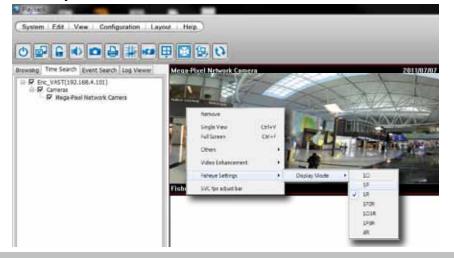
- 1. Launch an RTSP player.
- 2. Choose File > Open URL. A URL dialog box will pop up.
- 3. Type the above URL command in the address field.
- 4. The live video will be displayed in your player as shown below.



Open URL	
Enter on Internet URL to open rtsp://192.168.5.151:554/live.sdp	
	OK Cancel

NOTE:

An original, circular view will be displayed using all RTSP players. For access to the Regional Views, you can install VIVOTEK's ST7501 or VAST software. You can right-click on a live view



window to see the Display mode options.

RTSP port /RTP port for video, audio/ RTCP port for video, audio

- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

The ports can be changed to values between 1025 and 65535. The RTP port must be an even number and the RTCP port is the RTP port number plus one, and thus is always an odd number. When the RTP port changes, the RTCP port will change accordingly.

If the RTP ports are incorrectly assigned, the following warning message will be displayed:

Microsoft Internet Explorer 🛛 🛛			
1	Invalid port number. RTP video port must be an even number.		
	ОК		

<u>Multicast settings for stream 1 ~ 3</u>: Click the items to display the detailed configuration information. Select the Always multicast option to enable multicast for streams 1 ~ 3.

 Multicast settings for stream 1: Always multicast 	
Multicast group address:	239.128.1.99
Multicast video port:	5560
Multicast RTCP video port:	5561
Multicast audio port:	5562
Multicast RTCP audio port:	5563
Multicast TTL [1~255]:	15
 Multicast settings for stream 2: Always multicast 	
Multicast group address:	239.128.1.100
Multicast video port:	5564
Multicast RTCP video port:	5565
Multicast audio port:	5566
Multicast RTCP audio port:	5567
Multicast TTL [1~255]:	15

Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast group address and allows multiple clients to acquire the stream at the same time by requesting a copy from the multicast group address. Therefore, enabling multicast can effectively save Internet bandwith.

The ports can be changed to values between 1025 and 65535. The multicast RTP port must be an even number and the multicast RTCP port number is the multicast RTP port number plus one, and thus is always odd. When the multicast RTP port changes, the multicast RTCP port will change accordingly.

If the multicast RTP video ports are incorrectly assigned, the following warning message will be displayed:

Microso	ft Internet Explorer 🛛 🔀
♪	Invalid port number. Multicast stream 1 video port must be an even number.
	ОК

<u>Multicast TTL [1~255]</u>: The multicast TTL (Time To Live) is the value that tells the router the range a packet can be forwarded.

Initial TTL	Scope
0	Restricted to the same host
1	Restricted to the same subnetwork
32	Restricted to the same site
64	Restricted to the same region
128	Restricted to the same continent
255	Unrestricted in scope

Network > QoS (Quality of Service)

Quality of Service refers to a resource reservation control mechanism, which guarantees a certain quality to different services on the network. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. Quality can be defined as, for instance, a maintained level of bit rate, low latency, no packet dropping, etc.

The following are the main benefits of a QoS-aware network:

- The ability to prioritize traffic and guarantee a certain level of performance to the data flow.
- The ability to control the amount of bandwidth each application may use, and thus provide higher reliability and stability on the network.

Requirements for QoS

To utilize QoS in a network environment, the following requirements must be met:

- All network switches and routers in the network must include support for QoS.
- The network video devices used in the network must be QoS-enabled.

QoS models

CoS (the VLAN 802.1p model)

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates the frame priority level from 0 (lowest) to 7 (highest). The priority is set up on the network switches, which then use different queuing disciplines to forward the packets.

Below is the setting column for CoS. Enter the **VLAN ID** of your switch ($0\sim4095$) and choose the priority for each application ($0\sim7$).

- CoS	
Enable CoS	
VLAN ID:	1
Live video:	0 -
Live audio:	0 -
Event/Alarm:	0 -
Management:	0 -

If you assign Video the highest priority level, your network switch will handle video packets first.

D NOTE:

- ► A VLAN-capable Switch (802.1p) is required. Web browsing may fail if the CoS setting is incorrect.
- Class of Service technologies do not guarantee a level of service in terms of bandwidth and delivery time; they offer a "best-effort." Users can think of CoS as "coarsely-grained" traffic control and QoS as "finely-grained" traffic control.
- Although CoS is simple to manage, it lacks scalability and does not offer end-to-end guarantees since it is based on L2 protocol.

QoS/DSCP (the DiffServ model)

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Codepoint). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth, queueing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment; for example, how much bandwidth to reserve for it.

Below are the setting options of DSCP (DiffServ Codepoint). Specify the DSCP value for each application (0~63).

Enable QoS/DSCP		
Live video:	0	
Live audio:	0	
Event/Alarm:	0	
Management:	0	

Network > DDNS

This section explains how to configure the dynamic domain name service for the Network Camera. DDNS is a service that allows your Network Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name.

Express link

Express Link is a free service provided by VIVOTEK server, which allows users to register a domain name for a network device. One URL can only be mapped to one MAC address. This service will check out if the host name is valid and automatically open a port on your router. Unlike DDNS, which requires a user to manually check out details about UPnP port forwarding, the Express Link is more convenient and easy to set up.

Manual setup	Express link		
👿 Enable exp	oress link		
http://		.2bthere.net	Help Save
	ink, all users need to d amera from Internet.	o is create host name for the came	ra. It will generate the link to

Please follow the steps below to enable Express Link:

- 1. Make sure that your router supports UPnP port forwarding and it is activated, or you may see the following warning message: Express link is not supported under current network environment.
- 2. Check Enable express link.
- 3. Enter a host name for the network device and click **Save**. If the host name has been used by another device, a warning message will show up. If the host name is valid, it will show a message as shown below.

Enable express link	
http:// vivotek_test3454	.2bthere.net Help Save

"le Edit View Favorites Tools Hel	PSeedi 👷 "enstes 😧 🎯 - 🌺 📷 :	3
e) https://0002D1123456 2bther		
YVIVOTEK		Mega-Pixel Network
Video stream 1 -	(TCP.AV)	
Manual trigger Digital output On On	School and A	
Focus assist On OR		

Manual setup

DDNS: Dynamic domain name service

Manual setup	Express link		
Enable DD Provide		Dyndns.org(Dynamic)	
Host na]
User na Passw			
Hostina	ime:		[*.tzo.com]
Email: Key:			

Enable DDNS: Select this option to enable the DDNS setting.

Provider: Select a DDNS provider from the provider drop-down list.

VIVOTEK offers **Safe100.net**, a free dynamic domain name service, to VIVOTEK customers. It is recommended that you register **Safe100.net** to access VIVOTEK's Network Cameras from the Internet. Additionally, we offer other DDNS providers, such as Dyndns.org(Dynamic), Dyndns.org(Custom), TZO. com, DHS.org, CustomSafe100, dyn-interfree.it.

Note that before utilizing this function, please apply for a dynamic domain account first.

■ Safe100.net

- 1. In the DDNS column, select **Safe100.net** from the drop-down list. Click **I accept** after reviewing the terms of the Service Agreement.
- 2. In the Register column, fill in the Host name (xxxx.safe100.net), Email, Key, and Confirm Key, and click **Register**. After a host name has been successfully created, a success message will be displayed in the DDNS Registration Result column.

- Dogistor				
Register				
Host name:	WTK.safe100.net			
Email:	wtk@vivotek.com			
Key:	•••• Forget key			
Confirm key:	••••			
To apply for a domain name for the camera,	or to modify the previously registered information, fill in			
the following fields and then click "Register".				
Register				
DDNS registration result				
[Register] Successfully. Your account inform has been mailed to registered e-mail addre				
, Upon successful registration, you can click	copy to automatically upload relevant information to the			
DDNS form or you can manually fill it in. The	n, click "Save" to save new settings.			

3. Click **Copy** and all the registered information will automatically be uploaded to the corresponding fields in the DDNS column at the top of the page as seen in the following screen.

DDNS: Dynamic domain name service				
Imable DDNS				
Provider:	Safe100.net	•		
Host name:	wtk.safe100.net	[*.safe100.net]		
Email:	wtk@vivotek.com			
Key:	••••			
		Save		
Register				
Host name:	wtk.safe100.net			
Email:	wtk@vivotek.com			
Key:	••••	Forget key		
Confirm key:	••••			
To apply for a domain name for the came	ra, or to modify the prev	viously registered information,		
fill in the following fields and then click "Re	egister".			
Register				
DDNS registration result				
[Register] Successfully. Your account information has been mailed to registered e-mail address.				
Upon successful registration, you can clic	k <u>copy</u> to automaticall	y upload relevant information to		
the DDNS form or you can manually fill it in. Then, click "Save" to save new settings.				

4. Select Enable DDNS and click Save to enable the setting.

CustomSafe100

VIVOTEK offers documents to establish a CustomSafe100 DDNS server for distributors and system integrators. You can use CustomSafe100 to register a dynamic domain name if your distributor or system integrators offer such services.

- 1. In the DDNS column, select CustomSafe100 from the drop-down list.
- 2. In the Register column, fill in the Host name, Server name, Email, Key, and Confirm Key; then click **Register**. Enter "ns1.safe100.net" as the Server name.

After a host name has been successfully created, you will see a success message in the DDNS Registration Result column.

- 3. Click **Copy** and all for the registered information will be uploaded to the corresponding fields in the DDNS column.
- 4. Select Enable DDNS and click Save to enable the setting.

<u>Forget key</u>: Click this button if you have forgotten the key to Safe100.net or CustomSafe100. Your account information will be sent to your email address.

Refer to the following links to apply for a dynamic domain account when selecting other DDNS providers:

Dyndns.org(Dynamic) / Dyndns.org(Custom): visit http://www.dyndns.com/

Network > SNMP (Simple Network Management Protocol)

This section explains how to use the SNMP on the network camera. The Simple Network Management Protocol is an application layer protocol that facilitates the exchange of management information between network devices. It helps network administrators to remotely manage network devices and find, solve network problems with ease.

- The SNMP consists of the following three key components:
- 1. Manager: Network-management station (NMS), a server which executes applications that monitor and control managed devices.
- 2. Agent: A network-management software module on a managed device which transfers the status of managed devices to the NMS.
- 3. Managed device: A network node on a managed network. For example: routers, switches, bridges, hubs, computer hosts, printers, IP telephones, network cameras, web server, and database.

Before configuring SNMP settings on the this page, please enable your NMS first.

SNMP Configuration

Enable SNMPv1, SNMPv2c

Select this option and enter the names of Read/Write community and Read Only community according to your NMS settings.

Enable SNMPv1, SNMPv2c

SNMPv1, SNMPv2c Settings		
Read/Write community:	Private	
Read only community:	Public	

Enable SNMPv3

This option contains cryptographic security, a higher security level, which allows you to set the Authentication password and the Encryption password.

- Security name: According to your NMS settings, choose Read/Write or Read Only and enter the community name.
- Authentication type: Select MD5 or SHA as the authentication method.
- Authentication password: Enter the password for authentication (at least 8 characters).
- Encryption password: Enter a password for encryption (at least 8 characters).

Enable SNMPv3

SNMPv3 Settings		
Read/Write Security name:	Private	
Authentication Type:	MD5 🔽	
Authentication Password:		
Encryption Password:		
Read only Security name:	Public	
Authentication Type:	MD5 🗸	
Authentication Password:		
Encryption Password:		

Security > User Account

This section explains how to enable password protection and create multiple accounts.

Root Password					
	Root password	Privilege management	Account management		
	Root password:				
	Confirm root pass	word:		Save	

The administrator account name is "root", which is permanent and can not be deleted. If you want to add more accounts in the Manage User column, please apply the password for the "root" account first. 1. Type the password identically in both text boxes, then click **Save** to enable password protection.

- 2. A window will prompt for authentication; type the correct user's name and password in their respective
- fields to access the Network Camera.

Privilege management

Root passwor	d Privilege managem	ent Account management	
Allow anor	nymous viewing		
Operator:	Digital output	PTZ control	
Viewer:	Digital output	PTZ control	Save

<u>Digital Output & PTZ control</u>: You can modify the management privilege as operators or viewers. Select or de-select the checkboxes, and then click **Save** to enable the settings. If you give Viewers the privilege, Operators will also have the ability to control the Network Camera through the main page. (Please refer to Configuration on page 41).

<u>Allow anonymous viewing</u>: If you select this item, any client can access the live stream without entering a User ID and Password.

Account management				-
Account management	Root password	Privilege management	Account management	
	Existing user name	e:	Add new user	
	User name:			
	User password:			Delete
	Confirm user pass	word:		Add
	Privilege:		Administrator 🗨	Update
			Administrator Operator	
			Viewer	

Administrators can create up to 20 user accounts.

- 1. Input the new user's name and password.
- 2. Select the privilege level for the new user account. Click Add to enable the setting.

Access rights are sorted by user privilege (Administrator, Operator, and Viewer). Only administrators can access the Configuration page. Though operators cannot access the Configuration page, they can use the URL Commands to get and set the value of parameters. For more information, please refer to URL Commands of the Network Camera on page 134. Viewers access only the main page for live viewing.

Here you also can change a user's access rights or delete user accounts.

- 1. Select an existing account to modify.
- 2. Make necessary changes and click **Update** or **Delete** to enable the setting.

Security > HTTPS (Hypertext Transfer Protocol over SSL)

This section explains how to enable authentication and encrypted communication over SSL (Secure Socket Layer). It helps protect streaming data transmission over the Internet on higher security level.

Create and Install Certificate Method

Before using HTTPS for communication with the Network Camera, a **Certificate** must be created first. There are three ways to create and install a certificate:

Create self-signed certificate

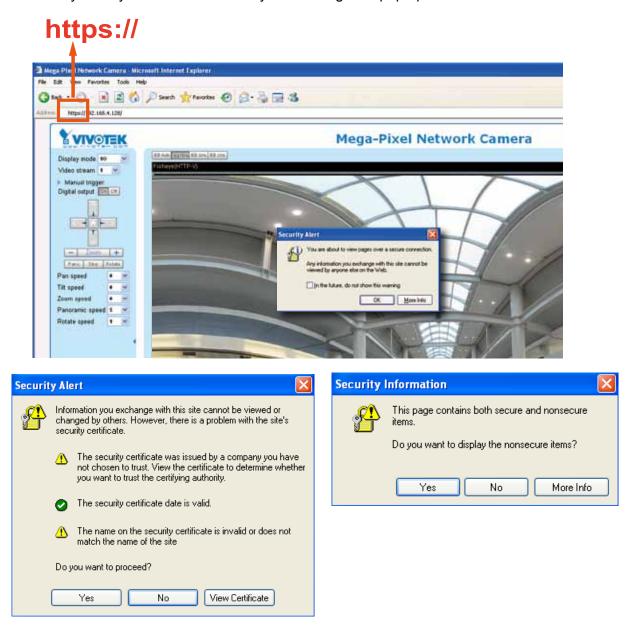
- 1. Select the first option.
- 2. Check **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
- 3. Click **Create certificate** to generate a certificate.

HTTP:	s —						
💽 Ena	able HTTPS secure cor	inection					
∞ Mo	de:						
	HTTP & HTTPS C	HTTPS only					
		, in the only					
₩ Ce	rtificate:						
	Certificate inform	ation					
	Status:		Not instal	ed			
	Method:		Create se	If-signed certificate	-		
	Country:		TW				
	State or province:		Asia				
Locality: Asia							
Organization: VIVOTEK Inc.							
	Organization unit:		VIVOTEK	Inc.			
	Common name:		www.viv	otek.com			
	Validity:		3650	days			
	1				Create ce	ertificate	
		Please wait wh generated	lie the certif	icate is being			

4. The Certificate Information will automatically be displayed in the lower screen as shown below. You can click **Certificate properties** to view detailed information about the certificate.

Certificate information	
Status:	Active
Method:	Create self-signed certificate
Country:	TW
State or province:	Asia
Locality:	Asia
Organization:	VIVOTEK Inc.
Organization unit:	VIVOTEK Inc.
Common name:	www.vivotek.com
	Certificate properties Remove certificate
	Save

- 5. Click **Save** to preserve your configuration, and your current session with the camera will change to the encrypted connection.
- 6. If your web session does not automatically change to an encrypted HTTPS session, click Home to return to the main page. Change the URL address from "<u>http://</u>" to "<u>https://</u>" in the address bar and press Enter on your keyboard. Some Security Alert dialogs will pop up. Click OK or Yes to enable HTTPS.



Create certificate request and install

- 1. Select the option from the **Method** pull-down menu.
- 2. Click Create certificate to proceed.
- 3. The following information will show up in a pop-up window after clicking **Create**. Then click **Save** to generate the certificate request.

Cer	tificate:	
	Certificate information	
	Status:	Notinstalled
	Method:	Create certificate request and install
	Country:	TW
	State or province:	Asia
	Locality:	Asia
	Organization:	VIVOTEK Inc.
	Organization unit:	VIVOTEK Inc.
	Common name:	www.vivotek.com
	Please wait while the certific generated	Create certificate

4. The Certificate request window will prompt.

	Create certificate request completed					
Copy the PEM format request below and send it to a CA for identify validation. After that, you have by clicking the "Upload" button on MTTPS page.						
Certificate request (PEM format)						
	BEGIN CERTIFICATE REQUEST					
	IIIN#20CAR#CAQI#CZELMAkGA1UEBHHOVTcxDTALBgHVNAgTBEF2#WExDTALBgHV					
	LeTREF##NE#FTATRgNUBA=TDFZJU#9020#gRNSjLjEVNBMCA1UEC#060%1WT12F					
	tyBJbeHuMRgwFgYDVQQDEw9343cudml2b3Rlay5jb2Dwg2EwDQYJKoZIhvcMAQEB IQADgYOAMIGJAcGBALfF5jkjh1CcufOHp43fOWUngGE9tQ8z1848CTbravhpun/W					
	D2JAYKHEhLQwGpmpsNy9erSYcu0JuG7bkhLAuHn/T97Rdv24UC0xGvmnSAg2SI6					
	mg12P75L244VnhusiccvvwR1VHCmX1xflouD2UERsc3UHpNL8x533r7vA5AgdB					
	AGdADANNgkghkiGWUBAQUFAA0BgQNdQgpKdU1cbwfd1RPnEU5HEMBnBriKNeQY					
	k/igITELX#PWESKAlgiSI4XpFNjXVRUs0Lw000h/myHDScJalxEZWiSJhD1A1Fm					
5	IXXNF1IAvC46aaCh5bqT5e9ILK6V11vC1pRXNmoEuUqNa4XYVyaRgd3aoeQuISVa					
5	Namrfluow==					
	END CERTIFICATE REQUEST					

If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.



5. Look for a trusted certificate authority, such as Symantec's VeriSign Authentication Services, that issues digital certificates. Sign in and purchase the SSL certification service. Copy the certificate request from your request prompt and paste it in the CA's signing request window. Proceed with the rest of the process as CA's instructions on their webpage.

ree Trial	► 25 Technical Cart	ent > 3 CSR > 1 Survivey		Chat With Us	1 2
Enter Certificate Signing	Request (CSR)				
Server platform: 🥥		Sample CS3		Order details	
Selectione	2	Alter der richten der Berlehen der B Berlehen der Berlehen der Berle Berlehen der Berlehen der B		Symmetries Th SSL Test Certill • Validity period: 30 aleys	ic.ex
		A DESCRIPTION OF A DESC	a Data Concervation Inc. Table Concervation	Total (Free Islat)	175 30
Paste Cettilicate Sign	ing Request (CSE)				
BOIN CERTIFICATE REQUEST				1 kilp	*
EACTOFYSIVE /TATBAYEACTOFYZ AVOLUTU/201052 EVIDENCA SUCCERENTATION SVBARMARIC // SVD/2020 / C300x2/m2401 cutrine (C5m2AR8a HAXOW/BALEP			What is a CSR?		
STOVHELDOZNÍCOU SPROUVHOVOMVEDANJE ALAMADOCSIOSED TREVENUL/USIOSED	LineDractionwood, WCeUth#Ib-Cda/Yoe CollegeLinA40BA0 Lin/DCyLlin/ThDidb #ITTMC0025040777	VIRSIN-EURILLINELLIN-SOBRENSON/SOLIGIA SOLOCIETTI-IN-INVENION CONSTRUCTION (INVESSION) CONSTRUCTION CONTROL (INVESSION) CONTROL (INVESSION) CONTROL (INVESSION) CONTROL (INVESSION) CONTROL (INVESSION) CON	-	A COR is generated from your your senser's unique "Ingers includes your senser's public entropy over sufferentiation communication head wild sense along a CORT or	rinf. The CSR say, which is and secure
				(0+++)	
		Intat 18 18 inter trial Clark Cancel	Continuet		

 Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solutions' UltraEdit.

immediately, please dial 866.893.6565 or 650.426.5113 option 3 or send an email to internet-sales@verisign.com
Thank you for your interest in Symantee!
BEOII CENTIFICATE HITFBOCCA-vgAx/HAgIQFx1Cahn/MEMSICNOCONIALNEHykghkiGMVORAQUFADCB yeELMAXGAIUEHNMCVNNCFAVNgKNRACTD11:m1TxMauLCBJmeMbHTMLgYUVQQL EydBD1qVRYACBQKKNAUEHCJGHTmuSLLAgTBOQTXHLGKJNHMILVYXQL EydBD1qVRYACBQKKNAUEHCJGHTmuSLLAgTBOQTXHLGKJNHMILVYXQL EydBD1qVRYACBQKKNAUEHCJGHTmuSLLAgTBOQTXHLGKJNHMILVYXQL EydBD1qVRYACBQKKNAUEHCJGHTMUSLLAGTBOQTXHLGKJNHMILVYXQL CalNgHTMATTAINXQVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV

7. Open a new edit, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.

fe Vene 🔷 🗰 🗙	· . · · · · · · · · · · · · · · · · · ·		* 8 ×
rotect Open Explorer Lists	Kditi x		
Rer: ** > D 5 By A: - C : -	Eddl* AD SE AD SE AD 18 CmcGBAGG+EUBBxUWHTAxBggrBgEFBgcCAPY3dHR0cHM6L93dBcudmVya3Np224 AD SE AD 19 CmcGBAGG+EUBBxUWHTAxBggrBgEFBgcCAPY3dHR0cHM6L93dBcudmVya3Np224 AD SE AD 19 Y296LENWeyF902XN072EWL0F0VF0F01BUTWFATIKW1DB0UHAWEGCcsGAQUFBwECBD0 AD AD AD 14 Y296LENWeyF902XN072EWL0F0VF0F01BUTWFATIKW19xND021AU739ERD4GCcsGAQUFBwEAB AD AD AD 15 BggrBgEFBgcwAYTYABR0cDovL29303AudwVyaXNp224u739ERD4GCcsGAQUFBwEAB AD AD AD 14 hjJodHRW010VU125VHJ9VWHERIEYVIhLn21cm1raWduLmNvb39TV1JUcm1hbEc LamNicsNot2004UHAS AD AD 15 JMSgkqhk169W05AUTAAOCAQEATNUHTFnise/X776c/zr:PEENhLK52G Ad AD AD AD 15 JMSgkqhk169W05AUTAAOCAQEATNUHTFnise/X776c/zr:PEENhLK52G AD AD		
		<u>بر</u>	

8. Convert file format from DOS to UNIX. Open **File** menu > **Conversions** > **DOS to Unix**.

-	Edit 1*] - UltraEdit Edit Search Insert Progr	vit Man Brane	Column Macro Scripting Advanced Window Help
3	lanv Open	CH+N CH+O	
	Quick Open Gloce Close All Files	Col+Q Col+Shift+F4	* 1 ×
10	Close All Files Except This	COMPARENTY	
	FTP/Televit Seve 3 Seve 3 Seve 4 Seve 4 Seve 5 Seve 4 Seve 5 Seve	, Co1+5 F12 Ak+F12 , Ak+F11	OSAGG+KURExUWTAVRggr BgEFHQcCARYjaHROCHKEL99103eudm/yaXNp224u tL2Nwcy902XNOY2EwHOYDVRDIDBYwFAYIKWYBDQUHAVEGCCGGAQUFFBwCHMBGG UwQYMBaFCgXE4g91qH134yst7a02hBwYG71HMQGCGGAQUFFBwCHBBG UBGFHQcwAYYYAHROCHOVL29jG3Audm/YgXNp224U29tHD4GCCGGAQUFFBxC dHBwO18VU125VHJpYWwtREItYUHLD1em1zmWzMSYSTVJJUzmihhEcy LcjANBgkqhk1G9wBAQUFAACCAQEATxuH7FnIae/X7T6z/zzr9zEKhLKSEQSp GSwixKe129p9ixEEXpf6TcLPHDcOG0fPalLFxAEUTTF29HIGCGWRIAjWp12 bDfxgVHWx9T7zd2oURzjmo6ifcH5Tzub3Qc2Tu3pWeAJDAH/U+x+ojGOEVB3z Shn/qcapKcqCXNHycwHeCWBBRQgsGe1368qXPzsw77GKrbnLhupjdxUES3CXu SCXrktQ2vHRadifJQYSTg5ONq2mk9ghdEuKTnhCHUwwqCxNBuceIIB3ITPK70 VyntblgmTzyJSEvgIUdc672Imm2B0q8c5q3i2AFPH/gi//XeGg== -KND_CERTIFICATE
	Conversions Special Functions	•	Control Marc to Dos To Dos to MAC
41114	Eynt Print All Files Print Preview Print Setup/Configuration	Col+P	
	Fagorite Hiles Recerk Files Recerk Frojects/WorkSpace	cod+shift+F	Additing CEM Power User
1	Est		Lawope to ASCII

	Save As				<u> ? ×</u>	1
	Savein	Desktop		000	3-	-
Name Date modified	My Recent Documents Decision Decision My Documents My Corputer	My Document My Computer My Natwork P Addus Reads P Fie2Bs Clenc Google Chron Distalation W CureClent Micrate Security Micration Sim Mocala Firefox P Rayback Si QuichTime Ris Readilyser Transflower d	laces 19 e Itorid 2 Ry Scan Has stect Smart Client 1 Yer		i大 (位於 Blackhole)	0H /6 =3 c1
	- 10	4			2	2
	My Nativest Places	File name: Save at type:	Al Files. (".")	1	Cancel	
		Line Terminator:	Default	3		-ċ
aut Windyn		Format:	Defait	💌		
		ADS Stream:		n for these extensions)		

9. Save the edit using the ".crt" extension, using a file name like "CAcert.crt."

10. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.

	Security > HTTPS	
System	- HTTPS	
Media	Enable HTTPS secure con	nection
Network	🛩 Mode:	
Security	C HTTP & HTTPS C	HTTPS only
User accounts	🛩 Certificate	
HTTPS	Certificate information	n
Access list	Status:	Walting for certificated
888 802, 1x	Select certificate file:	C/Documents and Se Drowse. Upload
PTZ	Method:	Create certificate request and install
Event	Country.	TW
Applications	State or province:	Asia
	Locality	Asia
Recording	Organization:	VIVOTEK Inc.
Local storage	Organization unit	VIVOTEK Inc.
	Common name:	www.vivolek.com
Banic mode]		Remove certificate

-

11. When the certifice file is successfully loaded, its status will be stated as **Active**. Note that a certificate must have been created and installed before you can click on the "**Save**" button for the configuration to take effect.

Wode:	
	TPS only
 Certificate: 	
Certificate information	
Status:	Active
Method	Create certificate request and install
Country:	TW
State or province:	Asia
Locality:	Asia
Organization	VIVOTEK Inc.
Organization unit	VIVOTEK Inc.
Common name:	www.vivotek.com
	Certificate properties Remove certificate

12.To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "<u>http://</u>" to "<u>https://</u>" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

Security Alert Image: Security Information Image: Weight of the secure connection. Ary infomation you exchange with this site cannot be viewed by anyone elie on the Weight of the warming Image: I				
In the page with this site cannot be viewed by anyone else on the Web. De you want to display the nonsecure items? Image with this site cannot be viewed by anyone else on the Web. De you want to display the nonsecure items? Image with this site cannot be viewed or change dby others. However, there is a problem with the site's security certificate was issued by a company you have not chose to trust. View the certifying authority. Image with this site cannot be viewed or change with the site certifying authority. Image with the security certificate was issued by a company you have not chose not trust. View the certifying authority. Image with the site certifying authority. Image with the site certificate was issued by a company you have not chose not trust. View the certificate is invalid or does not match the name of the site. De you want to proceed?	Security Alert		Security Information	
 Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate. The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority. The security certificate date is valid. The name on the security certificate is invalid or does not match the name of the site Do you want to proceed? 	Any information you exchange with this site viewed by anyone else on the Web.	cannot be	Do you want to display the n	onsecure items?
 changed by others. However, there is a problem with the site's security certificate. The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority. The security certificate date is valid. The name on the security certificate is invalid or does not match the name of the site Do you want to proceed? 	Securit	y Alert	X	
 not chosen to trust. View the certificate to determine whether you want to trust the certifying authority. The security certificate date is valid. The name on the security certificate is invalid or does not match the name of the site Do you want to proceed? 	£	changed by others. However, there is a prol security certificate.	blem with the site's	
The name on the security certificate is invalid or does not match the name of the site Do you want to proceed?		not chosen to trust. View the certificat you want to trust the certifying authorit	e to determine whether	
Do you want to proceed?			invelid or does not	
		match the name of the site	invalid of dues hot	
			ew Certificate	

Security > Access List

This section explains how to control access permission by verifying the client PC's IP address.

General Settings

 General settings			
Maximum number of concurrent streaming:	10 💌	Connection management	

<u>Maximum number of concurrent streaming connection(s) limited to</u>: Simultaneous live viewing for 1~10 clients (including stream #1, #2, and #3). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (IE Explorer or Quick Time Player).

<u>Connection management</u>: Click this button to display the connection status window showing a list of the current connections. For example:

	IP address	Elapsed time	User ID	
	192.168.1.147	12:20:34	root	
	61.22.15.3	00:10:09		
	192.168.3.25	45:00:34	greg	
		-		
Refresh Add to deny list Disconnect Close				

- IP address: Current connections to the Network Camera.
- Elapsed time: How much time the client has been at the webpage.
- User ID: If the administrator has set a password for the webpage, the clients have to enter a user name and password to access the live video. The user name will be displayed in the User ID column. If the administrator allows clients to link to the webpage without a user name and password, the User ID column will be empty.

There are some situations which allow clients access to the live video without a user name and password:

- 1. The administrator does not set up a root password. For more information about how to set up a root password and manage user accounts, please refer to Security > User account on page 88.
- 2. The administrator has set up a root password, but set **RTSP Authentication** to "disable". For more information about **RTSP Authentication**, please refer to RTSP Streaming on page 78.
- 3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing**, please refer to page 88.
- Refresh: Click this button to refresh all current connections.
- Add to deny list: You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please check Enable access list filtering and click Save in the first column.

Disconnect: If you want to break off the current connections, please select them and click this button. Please note that those checked connections will only be disconnected temporarily and will automatically try to re-link again (IE Explorer or Quick Time Player).

<u>Enable access list filtering</u>: Check this item and click **Save** if you want to enable the access list filtering function.

Filter

<u>Filter type</u>: Select **Allow** or **Deny** as the filter type. If you choose **Allow Type**, only those clients whose IP addresses are on the Access List below can access the Network Camera, and the others cannot access. On the contrary, if you choose **Deny Type**, those clients whose IP addresses are on the Access List below will not be allowed to access the Network Camera, and the others can access.

Then you can **Add** a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to Network > Enable IPv6 on page 73 for detailed information.

Filter	
Enable access list filtering	
Filter type: 🔘 Allow 💿 Deny	
IPv4 access list	
Add Delete	
IPv6 access list	
Add Delete	

There are three types of rules:

<u>Single</u>: This rule allows the user to add an IP address to the Allowed/Denied list. For example:

Filter address	
Rule: Single	
IP address:	
OK Cancel	

<u>Network</u>: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The routing prefix is written in CIDR notation. For example:

Filter address	
Rule: Network	
Network address / Network mask: 192.10	58.2.0 / 24
OK Cancel	

accesses from IP address 192.168.2.x will be bolcked.

If IPv6 filter is preferred, you will be prompted by the following window. Enter the IPv6 address and the two-digit prefix length to specify the range of IP addresses in your configuration.

Filter address	
Rule: Network	
Network address / Network mask:	1

Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List. Note: This rule is only applied to IPv4.

For example:

[Filter address
	Rule: Range 💌
	IP address - IP address: 192.168.2.0 - 192.168.2.255
	OK Cancel

Administrator IP address

<u>Always allow the IP address to access this device</u>: You can check this item and add the Administrator's IP address in this field to make sure the Administrator can always connect to the device.

Administrator IP address	
Always allow the IP address to access this device	
	Save

Security > IEEE 802.1x

Enable this function if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.

The 802.1x standard is designed to enhance the security of local area networks, which provides authentication to network devices (clients) attached to a network port (wired or wireless). If all certificates between client and server are verified, a point-to-point connection will be enabled; if authentication fails, access on that port will be prohibited. 802.1x utilizes an existing protocol, the Extensible Authentication Protocol (EAP), to facilitate communication.

■ The components of a protected network with 802.1x authentication:



- 1. Supplicant: A client end user (camera), which requests authentication.
- 2. Authenticator (an access point or a switch): A "go between" which restricts unauthorized end users from communicating with the authentication server.
- 3. Authentication server (usually a RADIUS server): Checks the client certificate and decides whether to accept the end user's access request.
- VIVOTEK Network Cameras support two types of EAP methods to perform authentication: EAP-PEAP and EAP-TLS.

Please follow the steps below to enable 802.1x settings:

- 1. Before connecting the Network Camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (i.e., MIS of your company) which can be validated by a RADIUS server.
- 2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).

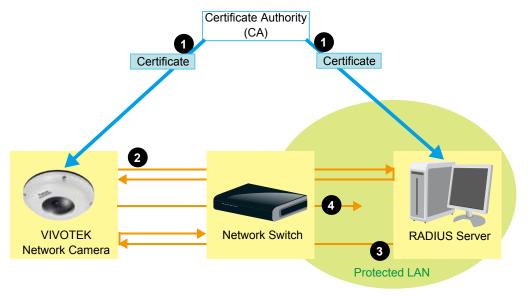
IEEE 802.1x			
Enable IEEE 802.1x		The maximum length	of password is 200
EAP method:	EAP-PEAP	symbols.	
Identity:			
Password:			
CA certificate:	Browse	Upload	
Status: no file	Remove		

- IEEE 802.1x	
Enable 802.1x	
EAP method:	EAP-TLS 🗸
Identity:	
Private key passord:	
CA certificate:	Browse Upload
Status: no file	Remove
client certificate:	Browse Upload
Status: no file	Remove
Client private key:	Browse Upload
Status: no file	Remove

3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.



- ► The authentication process for 802.1x:
- 1. The Certificate Authority (CA) provides the required signed certificates to the Network Camera (the supplicant) and the RADIUS Server (the authentication server).
- 2. A Network Camera requests access to the protected LAN using 802.1X via a switch (the authenticator). The client offers its identity and client certificate, which is then forwarded by the switch to the RADIUS Server, which uses an algorithm to authenticate the Network Camera and returns an acceptance or rejection back to the switch.
- 3. The switch also forwards the RADIUS Server's certificate to the Network Camera.
- 4. Assuming all certificates are validated, the switch then changes the Network Camera's state to authorized and is allowed access to the protected network via a pre-configured port.



PTZ > PTZ settings

This window is functional only when you configure a video stream to be using the Local dewarp function.

Changing the Field of View





In this window, functional items related to the preset positions have been cancelled. This window is now used for changing the field of view when the Local dewarp is applied to a video stream.

1. First select a video stream for which the field of view will take effect. Note that you must manually select a Local dewarp mode (e.g., 1R or 1P) in Media > Video window first.

(TCP-V)	2013/11/	26 16:26:30
A A	-	
the states	1 Starter	

2. Adjust the shooting area to the desired position using the PTZ keypad on the live screen.

Note that the pan, tilt, zoom speeds only applies in this window. They do not apply to the live view window.

Event > Event settings

This section explains how to configure the Network Camera to respond to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications. Click on **Help**, there is an illustration shown in the pop-up window explaining that an event can be triggered by many sources, such as motion detection or external digital input devices. When an event is triggered, you can specify what type of action that will be performed.

Name	Status Sun	Mon Tue V	Ved Thu	Fri Sat	Time	Trigger
Add	Help					close or Esc Key
			etection, Periodica put, System boot Media (What to send)	Server	(Where to send)
			Ex.	-	Ex.	

Event

An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window.

Enable this event ority: Normal
1. Schedule ✓ Sun Ø Mon Ø Tue Ø Wed Ø Thu Ø Fri Ø Sat Time ● Always ● From 00:00 to 24:00 [hh:mm]

- Event name: Enter a name for the event setting.
- Enable this event: Select this checkbox to enable the event setting.
- Priority: Select the relative importance of this event (High, Normal, or Low). Events with a higher priority setting will be executed first.
- Detect next event after seconds: Enter the duration in seconds to pause motion detection after a motion is detected. This prevents too many events to be triggered within a short time.

Follow the steps 1~3 to arrange the three elements -- Schedule, Trigger, and Action to set an event. A total of 3 event settings can be configured.

1. Schedule

Specify the period for the event. Please select the days of the week and the time in a day (in 24-hr time format) to specify when will the event-triggering conditions take effect.

2. Trigger

This is the cause or stimulus which defines what will trigger the event. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital inputs.

There are several choices of trigger sources as shown below. Select each item to display its related options.

Video motion detection

This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection on page 117 for details.

Video motion detection		
Normal: 🔲 door		
Profile: 📄 hallway		
Note: Please configure	Motion detection	irst

Periodically

This option allows the Network Camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.



Trigger every other 1 minutes

Digital input

This option allows the Network Camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices with digital input devices on the market which help detect changes in temperature, vibration, sound, light, etc.

System boot

This option triggers the Network Camera when the power to the Network Camera is disconnected.

Recording notify

This option allows the Network Camera to trigger when the recording disk is full or when recording starts to overwrite older data.

Audio detection

A preset threshold can be configured with an external microphone as the trigger to system event. The triggering condition can be an input exceeding or falling below a threshold. Audio detection can take place as a complement to motion detection or as a method to detect activities not covered by the camera's view.

Normal: Trigger event when detected audio	rises above 💌	alarm level
Profile: Trigger event when detected audio	rises above 💌	alarm level
Note: Please configure Audio detection first		

Once you have a preset audio alarm level, you can define the triggering condition either as an audio input rises above or falls below the alarm level.

Camera tampering detection

Audio detection

This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 120 for detailed information.

 Camera tamp 	ering de	tection
Enable cam	era tampo	ering detection
Trigger duration	10	seconds [10~600]

Manual Trigger

This option allows user to enable event triggers manually by clicking the on/off button on the homepage. Please configure $1 \sim 3$ events before using this function.





Save

VADP

These checkboxes allow the events to be triggered by 3rd-party software modules known as VADP. Users may implant these modules for different purposes such as triggering motion detection, or applications related to video analysis, etc. Please refer to page 123 for the configuration options with VADP modules.



0 1 2 3 4 5 6 7

3. Action Define the actions to be performed by the Network Camera when a trigger is activated.

	Action Action	nd(s).	
1. Schedule	Trigger digital output for 1	seconds	
	Backup media if the network	is disconnected	_
	Server Media	Extra parameter	
2. Trigger	SD snapshot 💌 S	<u>SD test</u> <u>View</u>	
	✓ NAS snapshot ✓	Create folders by date time and hour automaticall <u>View</u>	у
3. Action	Add server 💟 Add media		

■ Trigger digital output for □ seconds Select this option to turn on the external digital output device when a trigger is activated. Specify the length of the trigger interval in the text box.

Backup media if the network is disconnected Select this option to backup media file on SD card if the network is disconnected. Please note that this function will only apply after you set up the network storage (NAS). For more information about how to set up network storage, please refer to page 127.

To configure an event with video recording or snapshots, it is necessary to configure/provide servers and storage media settings so that the Network Camera will know where to send the media files to when a trigger is activated.

Add server

Click **Add server** to unfold the server setting window. You can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

There are four choices of server types available: Email, FTP, HTTP, and Network storage. Select the item to display the detailed configuration options. You can configure either one or all of them.

Add server Add media 오	
Server name: Email	
Server type	
Email	
Sender email address:	Camera@vivotek.com
Recipient email address:	VIVOTEK@vivotek.com
Server address:	Ms.vivotek.tw
User name:	
Password:	
Server port	25
This server requires a serv	ecure connection (SSL)
© FTP	
© HTTP	
Network storage	
Test	Close Save server

Server type - Email

Select to send the media files via email when a trigger is activated.

- Server name: Enter a name for the server setting.
- Sender email address: Enter a valid email address as the sender address.
- Recipient email address: Enter a valid email address as the recipient address.
- Server address: Enter the domain name or IP address of the email server.
- User name: Enter the user name of the email account if necessary.
- Password: Enter the password of the email account if necessary.
- Server port: The default mail server port is set to 25. You can also manually set another port.

If your SMTP server requires a secure connection (SSL), check **This server requires a secure connection (SSL)**.

To verify if the email settings are correctly configured, click **Test**. The result will be shown in a pop-up window. If successful, you will also receive an email indicating the result.

🗟 hay 17197 1585 1725 ya bada bada matariwa ngi - 👘 💽 🔯	🗿 hey 1997 i 101 5-121 hey-biologian (inderversing)
The email has been out raccessfully.	Eroc in sending email.
-	

Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

After you set up the first event server, a new item for event server will automatically appear on the Server list. If you wish to add more server options, click **Add server**.

Server	Media			Extra parameter				
SD	None 💌	<u>SD test</u>	<u>View</u>					
🔳 Email	None 💌							
Add server 🔍 Add media 🔍								

Server type - FTP

Select to send the media files to an FTP server when a trigger is activated.

Add server	Add media 🔽			
Server name:	FTP			
Server type				
Email				
FTP				
Server a	ftp.vivotek.vom			
Server p	21			
Userna	vivotek			
Passwo	•••••			
FTP fold				
V Pas	sive mode			
HTTP				
Network sto	orage			
	Test		Close	Save server

- Server name: Enter a name for the server setting.
- Server address: Enter the domain name or IP address of the FTP server.
- Server port: By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.
- User name: Enter the login name of the FTP account.
- Password: Enter the password of the FTP account.
- FTP folder name

Enter the folder where the media file will be placed. If the folder name does not exist, the Network Camera will create one on the FTP server.

Passive mode

Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

To verify if the FTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as shown below. If successful, you will also receive a test.txt file on the FTP server.

🚳 http://192.168.5.121/cgi-bin/admin/festserver.cgi 📰 🛅 🔀	🐴 http://192.160.5.121/cgi-bin/sdmin/tratserver.cgi 🗐 🛅 🔀
ftp transmission successfully,	ftp transmission failed.

Click **Save server** to enable the settings, then click **Close** to exit the Add server page.

Server type - HTTP

Select to send the media files to an HTTP server when a trigger is activated.

Add server	Add media 💟			
Server name:	HTTP			
Server type				
Email				
◎ FTP				
HTTP				
URL:		http://192	2.168.5.10/cgi-bi	n/upload.cgi
Usernan	ne:			
Passwor	d:			
Network stor	age			
	Test		Close	Save server

- Server name: Enter a name for the server setting.
- URL: Enter the URL of the HTTP server.
- User name: Enter the user name if necessary.
- Password: Enter the password if necessary.

To verify if the HTTP settings are correctly configured, click **Test**. The result will be shown in a pop-up window as below. If successful, you will receive a test.txt file on the HTTP server.

http://192.168.5.121/cgi-bin/admin/testserver.cgi - ... 🔳 🗖 🗙

🗿 http://192.168.5.121/cgi-bin/admin/testserver.cgi 🔳 🗖 🗙
HTTP Transmission failed.

Click **Save server** to enable the settings and click **Close** to exit the Add server page.

Network storage:

Select to send the media files to a network storage location when a trigger is activated. Please refer to **NAS server** on page 127 for details.

Click Save server to enable the settings, then click Close to exit the Add server page.

Action —					
📄 Trigger d	digital output for 1	se	conds		
Backup	media if the networ	k is disco	nnected		
Server	Media			Extra parameter	
SD	None	<u>SD test</u>	<u>View</u>		
🔲 Email	Snapshot Video clip				
FTP	System log				
HTTP	None 💌				
NAS	None 💌	Crea	te folders	by date time and h	our automatically
Add serve	er 🔍 Add med	lia 🔽			
				Close	Save event

SD Test: Click to test your SD card. The system will display a message indicating success or failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 130 for detailed information.

Add media

Click **Add media** to open the media setting window. You can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured. There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

Add server 💟 Add media
Media name: Snapshot
Media type
Attached media:
Snapshot
Source: Stream 1 💌
Send 1 pre-event image(s) [0~7]
Send 1 post-event image(s) [0~7]
File name prefix: Snapshot_
Add date and time suffix to file name
Video clip
System log
Close Save media

Media type - Snapshot

Select to send snapshots when a trigger is activated.

- Media name: Enter a name for the media setting.
- Source: Select to take snapshots from streams 1 ~ 3.
- Send □ pre-event images

The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

■ Send post-event images

Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

For example, if both the Send pre-event images and Send post-event images are set to 7, a total of 15 images are generated after a trigger is activated.

	1 pic.	2 pic.	3 pic.	4 pic.	5 pic.	6 pic.	7 pic.	8 pic.	9 pic.	10 pic.	11 pic.	10 pic.	12 pic.	13 pic.	14 pic.	15 pic.
	▲															
l						1	ſrigge	er Act	ivatic	n						

File name prefix

Enter the text that will be appended to the front of the file name.

Add date and time suffix to the file name. Select this option to add a date/time suffix to the file name. For example:



Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

After you set up the first media server, a new column for media server will automatically display on the Media list. If you wish to add more media options, click **Add media**.

	Server	Media	Extra parameter
	SD	None	<u>SD test</u> <u>View</u>
	NAS	Snapshot None 💌	Create folders by date time and hour automatically <u>View</u>
A	dd serve	er 👽 <u>Add med</u>	

Media type - Video clip

Select to send video clips when a trigger is activated.

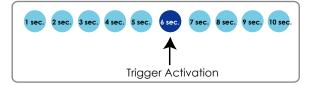
Add server 💟 Add media
Media name: Video Clip
Media type
Attached media:
Snapshot
Video clip
Source: Stream 1 💌
Pre-event recording: 0 seconds [0~9]
Maximum duration: 5 seconds [1~20]
Maximum file size: 500 Kbytes [50~6144]
File name prefix: Video
System log
Save media Close

- Media name: Enter a name for the media setting.
- Source: Select the source of video clip.
- Pre-event recording

The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds of video can be recorded.

Maximum duration

Specify the maximum recording duration in seconds. Up to 10 seconds of video can be recorded. For example, if pre-event recording is set to 5 seconds and the maximum duration is set to 10 seconds, the Network Camera continues to record for another 4 seconds after a trigger is activated.



Maximum file size Specify the maximum file size allowed.

File name prefix Enter the text that will be appended to the front of the file name. For example:

Video_20130720_100341							
\uparrow \uparrow							
File name prefix	Date and time suffix The format is: YYYYMMDD_HHMMSS						

Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

Media type - System log

Select to send a system log when a trigger is activated.

Add server 🔍 Add media	
Media name:	
Media type	
Attached media:	
Snapshot	
Video clip	
System log	
	Save media Close

Click **Save media** to enable the settings, then click **Close** to exit the Add media page.

Action —					
📄 Trigger dig	gital output for 1	se	conds		
🔲 Backup m	edia if the networ	k is disco	nnected		
Server	Media			Extra parameter	
				•	
SD -	None 🔻	<u>SD test</u>	View		
	Snapshot /ideo clip				
FTP	System log				
HTTP -	None 💌				
NAS -	None 💌	Crea <u>View</u>	te folders	by date time and ho	our automatically
Add server	Add med	ia 🔽			
				Close	Save event

- View: Click this button to open a file list window. This function is only for SD card and Network Storage. If you click View button of SD card, a Local storage page will pop up for you to manage recorded files on SD card. For more information about Local storage, please refer to page 130. If you click View button of Network storage, a file directory window will pop up for you to view recorded data on Network storage.
- Create folders by date, time, and hour automatically: If you check this item, the system will generate folders automatically by date.

The following is an example of a file destination with video clips:



Click to delete selected items

Click 20130320 to open the directory:



Click to open the file list for that hour

< 07 <u>08 09 10 11 12 13 14 15 16 17 ≥</u>									
file name size date time									
Video Clip_58.mp4	2526004	2013/03/20	07 <mark>:</mark> 58:28						
Video Clip_59.mp4	2563536	2013/03/20	07: <mark>59:</mark> 28						
Delete Delete all Back									
Click to delete Click to go back to the previous selected items level of the directory									
Click to delete all recorded data									

< 07 <u>08</u> <u>09</u>	<u>10 11</u>	12 13 14 1	<u>5 16 17 ></u>				
file na	me	size	date	time			
Video Clip_	58. np4	2526004	2013/03/20	07:58:28			
Video Clip_	59. <mark>np4</mark>	2563536	2013/03/20	07:59:28			
Delete all Back							

The format is: File name prefix + Minute (mm) You can set up the file name prefix on Add media page. Here is an example of the Event setting:

Enable this event Priority: Normal • Defect next motion detection or digital input after 10 second(s). Action • Action • Trigger digital output for 1 seconds • Backup media if the network is disconnected • SoNone• SO test Vaew • Create folders by date time and hour • False_NAS snapshots • automatically • View Add server • Add media • Media name: • So	Event name: intru_alar		1309
Detect neit motion detection or digital input after 10 second(s). 1. Schedule Trigger digital output for 1 seconds 2. Trigger Media Extra parameter 2. Trigger Media Extra parameter 3. Action False_NAS snapshots • automatically View Add server: • Add media Media name: Media name: Media name: Media type Attached media. • Snapshot • Snapshot • Week olip • System log • Stem log • Stem log		11	
1. Schedule 1. Schedule 2. Trigger 3. Action Trigger digital output for 1 seconds Image: SD Ima	Priority: Normal +		
1. Schedule 1. Schedule Image: Schedule	Detect next motion deter	tion or digital input after 10 second(s).	
1. Schedule Image: Server Media Extra parameter 2. Trigger Image: SD Image:		Action	
Image: Server Media Extra parameter 2. Trigger Image: SD None SD test Image: SD None SD test Yerx Image: SD Image: SD test Yerx Image: SD test Yerx Yerx Image: SD test Y		Trigger digital output for 1 seconds	
2. Trigger 2. Trigger 3. Action 3. Action 3. Action 4. Solarst Yaw Create folders by date time and hour Cr	1. Schedule	IV Backup media if the network is disconnected	
2. Trager 2. Trager 3. Action 4. Add server Add server Add media 5. Media type Attached media: 9. Snapshot 9. Video clip 9. System log		Server Media Extra parameter	
2. Trager 2. Trager 3. Action 4. Add server Add server Add media 5. Media type Attached media: 9. Snapshot 9. Video clip 9. System log	-	Z SDNone SD test View	
3. Action False_NAS snapshots • submatically Winw Add server • Add media Media name: Media name: Media type Atlached media. • Snapshot • Video dip • System log	2. Trigger		
3. Action Media name: Media name: Media type Attached media: Snapshot Video clip System log			ur.
3. Action Add server Add media Media name: Media type Attached media: Snapshot Video clip System log		V False_NAS snapshots 💌 automatically	
Media name: Media type Attached media: Snapshot Video clip System log	Same	View	
Media type Attached media: Snapshot Video clip System log	3. Action	Add server 🔾 Add media	
Media type Attached media: Snapshot Video clip System log			
Attached media: Snapshot Video clip System log		Media name:	
 Snapshot Video clip System log 		Media type	
 Video clip System log 		Attached media	
 Video clip System log 		O Snapshot	
System log			
Save media Close			
		Save media Cic	
Save event Close		Rang print / Pla	

When completed the settings with steps 1~3 to arrange Schedule, Trigger, and Action of an event, click **Save event** to enable the settings and click **Close** to exit the page.

The following is an example of the Event setting page:

Event —											
Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Trigger	
<u>intru alarm</u>	ON	v	v	v	v	V	v	v	00:00~24:00	motion	Delete
motiondetect	<u>ON</u>	۷	۷	۷	v	۷	v	۷	00:00~24:00	motion	Delete
Add	Hel	Ð									
Server setting	js —										
Name	Туре	;				Addr	ess/l	Locat	ion		
False NAS	ns									Delete	
Add											
Media ———											
vailable memo	ory space	e: 185	500KB								
Name		Туре	•								
snapshots	S	napsl	not								Delete
Add											
Customized	script										
Name		Date	•		Tim	e					
Add											

When the Event Status is <u>ON</u>, once an event is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

If you want to stop the event trigger, you can click <u>ON</u> to turn it to <u>OFF</u> status or click **Delete** to remove a previously-configured event setting.

To remove a server setting from the list, select a server name and click **Delete**. Note that only when the server setting is not being applied to an event setting can it be deleted.

To remove a media setting from the list, select a media name and click **Delete**. Note that only when the media setting is not being applied to an event setting can it be deleted.

Customized Script

This function allows you to upload a sample script (.xml file) to the webpage, which will save your time on configuring the settings. Please note that there is a limited number of customized scripts you can upload; if the current amount of customized scripts has reached the limit, an alert message will prompt. If you need more information, please contact VIVOTEK's technical support.

ſ	Customized	Script		_	
	Name	Date	Time		
	<u>User1</u>	20130413	18:13:46		
	User2	2013 0 413	18:11:32		
Click to upload a file	Add User1	Delete			
Click to modify the	schedule 1d="0"> duration> weekday>1-5c/weekday lume>05:30:00-20:30: /duration> /schedule> 1 Motion> motion condition="0" status 1d="0">trigge status 1d="0">trigge description>Mail sys condition>coschedulen>Odelay>10c/delay> 1 weers can send e f mail is the log me process>	02"> ccess risoroO on Monday to Fr coc/time> coc/ti	ess on" to recipient puddi	ng.yang@vivotek.com. The body g/measages -5 ms.vivotek.tw -	

Applications > Motion detection

This section explains how to configure the Network Camera to enable motion detection. A total of five motion detection windows can be configured.

2 Enable motion detection	
Pisheye(fCP-V) 2011//12 11 20 94 Window name nallway Sensithvity: 69% Percentage: 82% New Save	Motion Detection Setting 1: For normal situations
Profile	Motion Detection Setting 2: For special situations

Follow the steps below to enable motion detection:

- 1. Click New to add a new motion detection window.
- 2. In the Window Name text box, enter a name for the motion detection window.
 - Use four mouse clicks to define the area where Motion Detection will take effect.
 - To change the four points of the rectangular, place your mouse cursor on any of it until it turns into a four-direction mark
- 3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slide bar.
- 4. Click **Save** to enable the settings.
- 5. Select Enable motion detection to enable this function.

For example: I Enable motion detection

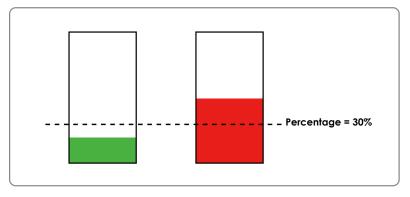


Profile

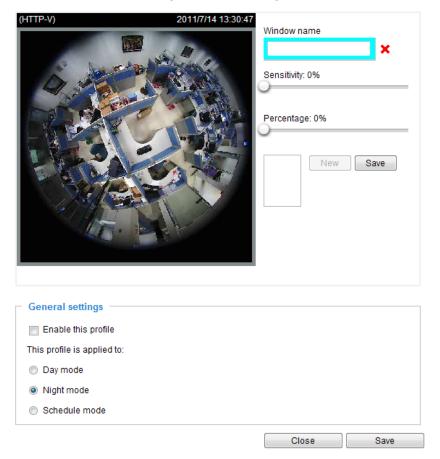
The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are considered to have exceeded the defined threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red. Photos or videos can be captured instantly and configured to be sent to a remote server (Email, FTP) using this feature as a trigger source. For more information on how to set an event, please refer to Event settings

on page 103.

A green bar indicates that even though motions have been detected, the event has not been triggered because the image variations still fall under the defined threshold.



If you want to configure specific motion detection settings individually for day/night/schedule operations, please click **Profile** to open the Motion Detection Profile Settings page as shown below. A total of three motion detection windows can be configured on this page as well.



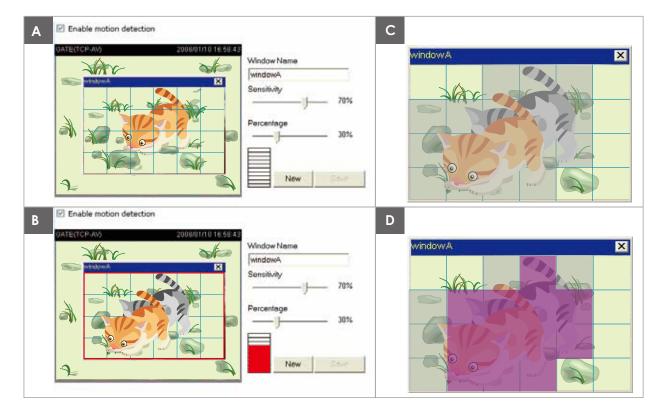
Please follow the steps beolw to set up a profile:

- 1. Create a new motion detection window.
- 2. Check Enable this profile.
- 3. Select the applicable mode: Day mode, Night mode, or Schedule mode. Please manually enter a time range if you prefer the Schedule mode.
- 4. Click **Save** to enable the settings and click **Close** to exit the page.

This motion detection window will also be displayed on the Event settings page. You can go to Event > Event settings > Trigger to choose it as a trigger source. Please refer to page 104 for detailed information.

NOTE:

► How does motion detection work?



There are two motion detection parameters: Sensitivity and Percentage. In the illustration above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray (frame C) and will be compared with the sensitivity setting. Sensitivity is a value that expresses the sensitivity to moving objects. Higher sensitivity settings are expected to detect slight movements while smaller sensitivity settings will neglect them. When the sensitivity is set to 70%, the Network Camera defines the pixels in the purple areas as "alerted pixels" (frame D).

Percentage is a value that expresses the proportion of "alerted pixels" to all pixels in the motion detection window. In this case, 50% of pixels are identified as "alerted pixels". When the percentage is set to 30%, the motions are judged to exceed the defined threshold; therefore, the motion window will be outlined in red.

For applications that require a high level of security management, it is suggested to use **higher** sensitivity settings and **smaller** percentage values.

Applications > DI and DO

Digital input		
Normal status:	High Cow	
Current status:	High	
Digital output		
Normal status:	🖲 Open 🔘 Grounded	
Current status:	Open	
		Save

<u>Digital input</u>: Select High or Low as the Normal status for the digital input. Connect the digital input pin of the Network Camera to an external device to detect the current connection status.

<u>Digital output</u>: Select Grounded or Open to define the normal status for the digital output. Connect the digital output pin of the Network Camera to an external device to determine the current status.

Set up the event source as DI on **Event > Event settings > Trigger.** Please refer to page 104 for detailed information.

Applications > Tampering detection

This section explains how to set up camera tamper detection. With tamper detection, the camera is capable of detecting incidents such as **redirection**, **blocking or defocusing**, or even **spray paint**.

 Camera tampe 	ering de	tection	
Enable came	era tamp	ering detection	
Trigger duration	10	seconds [10~600]	
			Save

Please follow the steps below to set up the camera tamper detection function:

1. Check Enable camera tampering detection.

- 2. Enter the tamper trigger duration. (10 sec. ~ 10 min.) The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.
- 3. Set up the event source as Camera Tampering Detection on **Event > Event settings > Trigger.** Please refer to page 104 for detailed information.

Applications > Audio detection

Audio detection, along with video motion detection, is applicable in the following scenarios:

- 1. Detection of activities not covered by camera view, e.g., a loud input by gun shots or breaking a door/window.
- A usually noisy environment, such as a factory, suddenly becomes quiet due to a breakdown of machines.
- 3. A PTZ camera can be directed to turn to a preset point by the occurrence of audio events.
- 4. Dark environments where video motion detection may not function well.

90				Alarm Leve
80		-	1	
60	0.0	(
50	12		Tun	
40				
20				
10				
0				

The red circles indicate where the audio alarms can be triggered when breaching or falling below the preset threshold.

How to configure Audio detection:

- 1. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.
- 2. Use a mouse click to drag the Alarm level tab to a preferred location on the slide bar.
- 3. Select the "Enable audio detection" checkbox and click Save to enable the feature.

NOTE:

- 1. Note that the volume numbers (0~100) on the side of wave diagram does not represent decibel (dB). Sound intensity level has already been mapped to preset values. You can, however, use the real-world inputs at your installation site that are shown on the wave diagram to configure an alarm level.
- 2. To configure this feature, you must not mute the audio in **Configuration > Media > Audio**. The default of the camera can be muted due to the lack of an internal microphone. An external microphone is provided by users.

You can use the **Profile** window to configure a different Audio detection setting. For example, a place can be noisy in the day time and become very quiet in the night.

- 1. Click on the **Enable this profile** checkbox. Once the Audio detection window is opened, the current sound input will be interactively indicated by a fluctuating yellow wave diagram.
- 2. Use a mouse click to drag the Alarm level tab to a preferred location on the slide bar.
- 3. Select the **Day**, **Night**, or **Schedule** mode check circles. You may also manually configure a period of time during which this profile will take effect.
- 4. Click **Save** and then click **Close** to complete your configuration.

	100	Alarm Level
	90	Volume
	80	
	70	
	60	
	50	
	40	
	30	
	20	
	10	
	eral settings	
his	profile is applied to:	
	Day mode	
1 (Night mode	
	Schedule mode	
9)5		



IMPORTANT:

- If the Alarm level and the received volume are set within a range of 20% on the wave diagram, frequent alarms will be triggered. It is recommended to set the Alarm level farther apart from the detected sound level.
- To configure and enable this feature, you must not configure video stream #1 into Motion JPEG. If an external microphone input is connected and recording of audio stream is preferred, audio stream is transmitted between camera and viewer/recording station along with stream #1.
- Refer to page 68 for Audio settings, and page 63 for video streaming settings.

Applications > VADP (VIVOTEK Application Development Platform)

Upload package —					
Save to SD card					
Select file			Brov	vse U	pload
Resource status					
🐭 Storage status:					
storage_size:	10240 KByte	s Free s	ize:	10240 KBy	rtes
* SD card status: De	etached				
Total size:	0 KBytes	Free size:	:	0 KBytes	
Used size:	0 KBytes	Use (%):		0 %	
🐭 Memory status:					
Total size:	24576 KBytes	Free size	e: 2	4576 KByt	es
— Module list —					
Module na	me	Vendor	Version	Status	License
Backup	Reload	lestore	Start	Sto	qq

Users can store and execute VIVOTEK's or 3rd-party software modules onto the camera's flash memory or SD card. These software modules can apply in video analysis for intelligent video applications such as license plate recognition, object counting, or as an agent for edge recording, etc.

- Once the software package is successfully uploaded, the module configuration (vadp.xml) information is displayed. When uploading a module, the camera will examine whether the module fits the predefined VADP requirements. Please contact technical support or the vendor of your 3rd-party module for the parameters contained within.
- Users can also run VIVOTEK's VADP packages as a means to access updated functionality instead of replacing the entire firmware.
- Note that for some cameras the flash is too small to hold VADP packages. These cameras will have its "Save to SD card" checkbox selected and grayed-out for all time.
- The file system of SD card (FAT32) does not support soft (symbolic) link. It will return failure if your module tries to create soft links on SD card.

To utilize a software module, acquire the software package and click **Browse** and **Upload** buttons. The screen message for a successful upload is shown below:



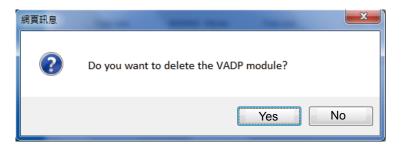
To start a module, select the checkcircle in front, and click the **Start** button.

– Mo	dule list –					
	Modu	le name	Vendor	Version	Status	License
0	Hello	World	ABC	3.8.24	ON	yes
	Backup	Reload	Restore	Start	Sto	p

If you should need to remove a module, select the checkcircle in front and then click the **Stop** button. By then the module status will become **OFF**, and the **X** button will appear at the end of the row. Click on the **X** button to remove an existing module.

Module list										
	Modu	le name	Vendor	Version	Status	License				
	Hello World		ABC	3.8.24	Off	yes	88			
	Backup	Reload	Restore	Start	Sto	p				

When prompted by a confirm message, Click Yes to proceed.



Note that the actual memory consumed while operating the module will be indicated on the **Memory status** field. This helps determine whether a running module has consumed too much of system resources.

Recording > Recording settings

This section explains how to configure the recording settings for the Network Camera.

Recording Settings

			In	sert	your	SD card a	nd click	here to test	
- Recordi	ng settings -								
Name 9	Status Sun M	on Tue W	ed Thu	Fri	Sat	Time	Source	Destination	Delete
Add	<u>SD te</u>	<u>st</u>							

NOTE:

Please remember to format your SD card when used for the first time. Please refer to page 130 for detailed information.

Recording Settings

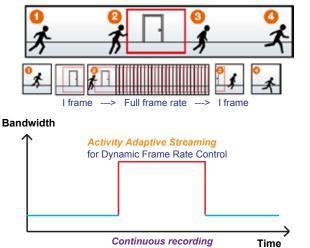
Click **Add** to open the recording setting window. On this page, you can define the adaptive recording, recording source, recording schedule, and recording capacity. A total of 2 recording settings can be configured

mguleu.	Recording name: Video	
	👿 Enable this recording	l
	👿 With adaptive recordi	ng
	Pre-event recordir	ng: 5 seconds [0~9]
	Post-event record	ing: 5 seconds [0~10]
	Priority: Normal 💌	
	Source: Stream 1 💌	
		Trigger
	1. Trigger	Schedule
		🖉 Sun 🖉 Mon 👽 Tue 👽 Wed 👽 Thu 👽 Fri 👽 Sat
		Time
	•	Always
	2. Destination	From 00:00 to 24:00 [hh:mm]
		Network fail
	Note: To enable recording	g notification please configure <u>Event</u> first
		Close Save

- Recording name: Enter a name for the recording setting.
- Enable this recording: Select this option to enable video recording.
- With adaptive recording:

Select this option will activate the frame rate control according to alarm trigger. The frame control means that when there is a triggered alarm/event, the frame rate will raise up to the value you've set on the Stream setting page. Please refer to page 63 for more information.

If you enable adaptive recording on Camera A, only when an event is triggered on Camera A will the server record the streaming data in full frame rate; otherwise, it will only request the I frame data during normal monitoring, thus effectively save lots of bandwidths and storage.





- To enable adaptive recording, please make sure you've set up the triggering sources such as Motion Detection, DI Device, or Manual Trigger.
- When there is no alarm trigger:
 JPEG mode: record 1 frame per second.
 - H.264 mode: record the I frame only.
 - MPEG-4 mode: record the I frame only.
- When the Intra frame period has been set to larger than >1s on Video settings page, the Intra frame period will be forced into 1s when the adaptive recording is activated.

The alarm trigger includes: motion detection and DI detection. Please refer to Event settings on page 103.

- Pre-event recording and post-event recording The Network Camera has a buffer area; it temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before and after a trigger is activated.
- Priority: Select the relative importance of this recording (High, Normal, or Low). Recording with a higher priority setting will be executed first.
- Source: Select a stream for the recording source.



- To enable adaptive recording, please also enable time shift caching stream and select a caching stream on Media > Video > Stream settings. Please refer to page 63 for detailed instruction.
- ► To enable recording notification please configure *Event settings* first. Please refer to page 103.

Please follow steps 1~2 below to set up the recording:

1. Trigger

Select a trigger source.

r Trigger
i i i ggei
Schedule
🖉 Sun 🖉 Mon 🖉 Tue 👽 Wed 👽 Thu 🖉 Fri 👽 Sat
Time
Always
From 00:00 to 24:00 [hh:mm]
Network fail

- Schedule: The server will start to record files on the local storage or network attached storage (NAS).
- Network fail: Since network fail, the server will start to record files onto the local storage (SD card).

2. Destination

You can select the SD card or network storage (NAS) for the recorded video files.

g (Helg)			
Maximum duration: 1	nt ranutes (1-60)		
Add NAS server	MB [100-2000]		
	Destination Destination: SD - Recording file managemen Maximum duration: 1 Maximum file size: 100	Destination: SD - Destination: SD - Recording file management Maximum duration: 1 nextee (1~60) Maximum file size 100 MB (100-2000)	Destination: 30 - Recording file management Maximum duration: 1 neutee (1-40) Maximum file size: 100 MB (100-2000)

NAS server

Click Add NAS server to open the server setting window and follow the steps below to set up:

- 1. Fill in the information for the access to the shared networked storage.
 - For example:

	Add NAS server				
	Server name: Server type	NAS		orage path ame or IP add	dress\folder name)
1	Network sto Network	rage storage location:	\\192.	160.5.122\nas	
	(For exar	mple: \\my_nas\disk\f	older)		
	Workgro	up:	vivote	k	
	User nar	me:	ritali		User name and password for your
	Passwor	rd:	••••	••	server
		Test		Save server	Close
		2		4	

2. Click **Test** to check the setting. The result will be shown in the pop-up window.

🗿 http://192.168.5.151/cgi-bin/admin/testserver 🔳 🗖 🔀	🗿 http://192.168.5.151/cgi-bin/admin/testserver 🗐 🗖 🔀
Mount succeeded.	Mount failed.
🗃 Done 🔹 🔮 Internet	🗃 Done

🗟 NAS on ritali - IC X File Edit View Favorites Tools Help 🔇 Back 🔻 🕥 🕤 🏂 🔎 Search 🛛 Folders 🛛 🞹 🗸 Address 🧟 \\ritali\NAS 💌 🔁 Go test.txt * File and Folder Tasks -Text Document 1 KB 📺 Rename this file 🙆 Move this file 📕 test.txt - Notepad Copy this file File Edit Format View Help 🔕 Publish this file to the Web [NOTIFICATION] The Result of Server Test of Your IP Camera 😒 E-mail this file 🍓 Print this file 🗙 Delete this file * Other Places

If successful, you will receive a test.txt file on the networked storage server.

- 3. Enter a server name.
- 4. Click **Save** to complete the settings and click **Close** to exit the page.

Enable this recording		٠
With adaptive recording	(<u>Help</u>)	
Priority: Normal 💌		
Source: Stream 1 💌		
[Destination	
1. Trigger	Destination: NAS 💌	
	Capacity:	
	Entire free space	
	Reserved space: 100 Mbytes	
2. Destination	Enable cyclic recording	E
	Recording file management	
	Maximum duration: 1 minutes [1~60]	
	Maximum file size: 100 MB [100~2000]	
	File name prefix: Bahasa	
Note: To opphie recording pr	otification please configure <u>Event</u> first	
Note. To enable recording in	Save Close	
	Gave Close	+

- Capacity: You can either choose the entire available space or impose a reserved space. The **Reserved** space should be of the size of at least **15MBytes**. The reserved space can be used as a safe buffer especially when the cyclic recording function is enabled, during the transaction stage when a storage space is full and the incoming streaming data is about to overwrite the previously saved videos.
- File name prefix: Enter the text that will be appended to the front of the file name.
- Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one.

Recording file management

- Maximum duration: This determines the length of each recorded video, applicable from 1 to 60 minutes.
- Maximum file size: This determines the file size of each concluded recording. The applicable sizes

range from 100 to 2000 Megabytes.

File name prefix: Enter a name for each recorded video.

If you want to enable recording notification, please click **<u>Event</u>** to set up. Please refer to **Event > Event** settings on page 103 for more details.

When completed, select **Enable this recording**. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the network storage or SD card. The new recording name will appear on the recording page as shown below.

To remove an existing recording setting from the list, single-click to select it and click **Delete**.

- Recor	ding set	tting	s —									
Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete
Video	ON	۷	V	۷	V	۷	۷	V	00:00~24:00	stream1	<u>SD</u>	Delete
A	dd	<u>s</u>) test									

- Video (Name): Click to open the Recording settings page to modify.
- ON (Status): Click to manually adjust the Status. (ON: start recording; OFF: stop recording)
- NAS or SD (Destination): Click to open the file list of recordings as shown below. For more information about folder naming rules, please refer to page 114 for details.

Local storage > SD card management

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, and implement SD card control.

SD card staus

This column shows the status and reserved space of your SD card. Please remember to format the SD card when using for the first time.

SD card status				
SD card status:	Detached	no SD	card	
Total size:	C	KBytes	Free size:	0 KBytes
Used size:	C) KBytes	Use (%):	0 %
				Format
SD card status				
SD card status:	Ready			
Total size:	7	810152 KBytes	Free size:	7602048 KBytes
Used size:	2	08104 KBytes	Use (%):	2.665 %
				Format

SD card control

- SD card control			
Enable cyclic storage			
Enable automatic disk cleanup			
Maximum duration for keeping files:	7	days	
			Save

- Enable cyclic storage: Check this item if you want to enable cyclic recording. When recording uses up all capacity, the oldest file will be overwritten by the latest file.
- Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter "7 days", the recorded files will be stored on the SD card for 7 days.

When all settings are completed, click **Save** to enable your settings.

Local storage > Content management

This section explains how to manage the content of recorded videos on the Network Camera. Here you can search and view the records and view the searched results.

Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click **Search** button, all recorded data will be listed in the **Search Results** cloumn.

Searching and viewing the records								
✤ File attributes								
Trigger type:	System boot	Recording notify Motion						
	📄 Digital input	Network fail						
	📄 Manual trigge	ers 🔲 Tampering detection						
	Audio detection	n						
Media type:	Video clip	Snapshot Text						
Locked:	Locked	Unlocked						
Backup:	Backup							
👻 Trigger time								
From:	Date	Time						
to:	Date	Time						
	(yyyy-mm-do	d) (hh:mm:ss)						
		Search						

- File attributes: Select one or more items as your search criteria.
- Trigger time: Manually enter the time range you want to search.

Click **Search** and the recorded data corresponding to the search criteria will be listed in **Search Results** window.

Search Results

The following is an example of search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click to sort the search results in either direction.

on on	ers of entri e page	es displaye	d	Enter a l search r	key word to esults	o filter the
Show 1			s	Search:		
	Trigger time 🔷	Media Type 🍦	Trigger type 🍦	Locked 🌲	Backup 🖕	Highlight an item
	2010-08-26 10:42:55	Video Clip	Periodically	No	No	
	2010-08-26 10:43:56	Video Clip	Periodically	No	No	
	2010-08-26 10:44:56	Video Clip	Periodically	No	No	
	2010-08-26 10:45:57	Video Clip	Periodically	No	No	
	2010-08-26 10:46:58	Video Clip	Periodically	No	No	
	2010-08-26	Video Clip	Periodically	No	No	

View: Click on a search result which will highlight the selected item in purple as shown above. Click the View button and a media window will pop up to play back the selected file. For example:



Click to select the Display mode

Click to adjust the image size

Download: Click on a search result to highlight the selected item in purple as shown above. Then click the **Download** button and a file download window will pop up for you to save the file.

- JPEGs to AVI: This function only applies to "JPEG" format files such as snapshots. You can select several snapshots from the list, then click this button. Those snapshots will be converted into an AVI file.
- Lock/Unlock: Select the desired search results, then click this button. The selected items will become Locked, which will not be deleted during cyclic recoroding. You can click again to unlock the selections. For example:

Show	10 💽 entries			Search:		
	Trigger time 🛛 🍦	Media type	Trigger type	Locked	🔷 Backup 🌲	
V	2012-07-11 17:56:12	Video clip	Boot	Yes	No	
V	2012-07-11 17:35:10	Snapshot	Boot	Yes	No	
V	2012-07-11 17:35:10	Snapshot	Boot	Yes	No	
	2012-07-11 17:35:10	Snapshot	Boot	No	No	
	2012-07-11 17:35:10	Snapshot	Boot	No	No	
	2012-07-11 17:35:10	Snapshot	Boot	No	No	Click to browse
Showing	g 1 to 6 of 6 entries				~ >	pages
View	Download	JPEGs to AV	1 Lock/Unlock	Remove		_
ote: "Vie	ew" and "Download" o	only apply to the I	nighlight item			

■ Remove: Select the desired search results, then click this button to delete the files.

Appendix URL Commands for the Network Camera

1. Overview

For some customers who already have their own web site or web control application, the Network Camera/Video Server can be easily integrated through URL syntax. This section specifies the external HTTP-based application programming interface. The HTTP-based camera interface provides the functionality to request a single image, control camera functions (PTZ, output relay etc.), and get and set internal parameter values. The image and CGI-requests are handled by the built-in Web server.

2. Style Convention

In URL syntax and in descriptions of CGI parameters, text within angle brackets denotes content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets should also be replaced. An example of this is the description of the name for the server, denoted with <servername> in the URL syntax description below, that is replaced with the string myserver in the URL syntax example further down in the page.

URL syntax is denoted with the word "Syntax:" written in bold face followed by a box with the referenced syntax as shown below. For example, name of the server is written as <servername> and is intended to be replaced with the name of the actual server. This can either be a name, e.g., "mywebcam" or "thecam. adomain.net" or the associated IP number for the server, e.g., 192.168.0.220.

Syntax:

http://<servername>/cgi-bin/viewer/video.jpg

Description of returned data is written with "**Return:**" in bold face followed by the returned data in a box. All data is returned in HTTP format, i.e., each line is separated with a Carriage Return and Line Feed (CRLF) printed as \r\n. Return:

HTTP/1.0 <HTTP code> <HTTP text>\r\n

URL syntax examples are written with "**Example:**" in bold face followed by a short description and a light grey box with the example.

Example: request a single snapshot image

http://mywebserver/cgi-bin/viewer/video.jpg

3. General CGI URL Syntax and Parameters

CGI parameters are written in lower-case and as one word without any underscores or other separators. When the CGI request includes internal camera parameters, these parameters must be written exactly as they are named in the camera or video server. The CGIs are organized in functionally-related directories under the cgi-bin directory. The file extension .cgi is required.

Syntax:

http://<*servername*>/cgi-bin/<*subdir*>[/<*subdir*>...]/<*cgi*>.<*ext*> [?<parameter>=<value>[&<parameter>=<value>...]]

Example: Set digital output #1 to active

http://mywebserver/cgi-bin/dido/setdo.cgi?do1=1

4. Security Level

SECURITY LEVEL	SUB-DIRECTORY	DESCRIPTION
0	anonymous	Unprotected.
1 [view]	anonymous, viewer,	1. Can view, listen, talk to camera.
	dido, camctrl	2. Can control DI/DO, PTZ of the camera.
4 [operator]	anonymous, viewer,	Operator access rights can modify most of the camera's
	dido, camctrl, operator	parameters except some privileges and network options.
6 [admin]	anonymous, viewer,	Administrator access rights can fully control the camera's
	dido, camctrl, operator,	operations.
	admin	
7	N/A	Internal parameters. Unable to be changed by any external
		interfaces.

5. Get Server Parameter Values

Note: The access right depends on the URL directory. **Method:** GET/POST

Syntax:

http://<*servername*>/cgi-bin/anonymous/getparam.cgi?[<*parameter*>] [&<parameter>...]

http://<servername>/cgi-bin/viewer/getparam.cgi?[<parameter>]

[&<parameter>...]

http://<*servername*>/cgi-bin/operator/getparam.cgi?[<*parameter*>] [&<parameter>...]

http://<*servername*>/cgi-bin/admin/getparam.cgi?[<*parameter*>] [&<parameter>...]

Where the *<parameter>* should be *<group>*[_*<name>*] or *<group>*[.*<name>*]. If you do not specify any parameters, all the parameters on the server will be returned. If you specify only *<group>*, the parameters of the related group will be returned.

When querying parameter values, the current parameter values are returned.

A successful control request returns parameter pairs as follows:

Return:

1TTP/1.0 200 OK\r\n	
Content-Type: text/html\r\n	
Context-Length: <length>\r\n</length>	
,r\n	
<pre><parameter pair=""></parameter></pre>	
where <parameter pair=""> is</parameter>	
<parameter>=<value>\r\n</value></parameter>	

[<parameter pair>]

<length> is the actual length of content.

Example: Request IP address and its response

Request: http://192.168.0.123/cgi-bin/admin/getparam.cgi?network_ipaddress

Response: HTTP/1.0 200 OK\r\n Content-Type: text/html\r\n Context-Length: 33\r\n \r\n network.ipaddress=192.168.0.123\r\n

6. Set Server Parameter Values

Note: The access right depends on the URL directory. **Method:** GET/POST

Currheum
Syntax:
http://< <i>servername</i> >/cgi-bin/anonymous/setparam.cgi? < <i>parameter</i> >=< <i>value</i> >
[& <parameter>=<value>][&update=<value>][&return=<return page="">]</return></value></value></parameter>
http://< <i>servername</i> >/cgi-bin/viewer/setparam.cgi? < <i>parameter</i> >= <value></value>
[& <parameter>=<value>][&update=<value>] [&return=<return page="">]</return></value></value></parameter>
http:// <servername>/cgi-bin/operator/setparam.cgi? <parameter>=<value></value></parameter></servername>
[& <parameter>=<value>][&update=<value>] [&return=<return page="">]</return></value></value></parameter>
http://< <i>servername</i> >/cgi-bin/admin/setparam.cgi? < <i>parameter</i> >=< <i>value</i> >
[& <parameter>=<value>][&update=<value>] [&return=<return page="">]</return></value></value></parameter>

PARAMETER	VALUE	DESCRIPTION		
<pre><group>_<name> value to assigned</name></group></pre>		Assign <value> to the parameter <group>_<name>.</name></group></value>		
update	<boolean></boolean>	Set to 1 to update all fields (no need to update parameter in		
		each group).		
return	<return page=""></return>	Redirect to the page < return page > after the parameter is		
		assigned. The < <i>return page</i> > can be a full URL path or relative		
		path according to the current path. If you omit this parameter, it		
		will redirect to an empty page.		
		(Note: The return page can be a general HTML file (.htm, .html)		
		or a VIVOTEK server script executable (.vspx) file. It cannot be		
		a CGI command or have any extra parameters. This parameter		
		must be placed at the end of the parameter list		

Return: HTTP/1.0 200 OK\r\n Content-Type: text/html\r\n Context-Length: <length>\r\n \r\n <*parameter pair*>

where <parameter pair> is

<parameter>=<value>\r\n

[<parameter pair>]

Only the parameters that you set and are readable will be returned.

Request: http://myserver/cgi-bin/admin/setparam.cgi?network_ipaddress=192.168.0.123 Response: HTTP/1.0 200 OK\r\n Content-Type: text/html\r\n Content-Type: text/html\r\n Context-Length: 33\r\n \r\n network.ipaddress=192.168.0.123\r\n

7. Available parameters on the server

Valid values:

VALID VALUES	DESCRIPTION
string[<n>]</n>	Text strings shorter than `n' characters. The characters ``,', <,>,& are invalid.
string[n~m]	Text strings longer than `n' characters and shorter than `m' characters. The
	characters ",', <,>,& are invalid.
password[<n>]</n>	The same as string but displays `*' instead.
integer	Any number between $(-2^{31} - 1)$ and $(2^{31} - 1)$.
positive integer	Any number between 0 and $(2^{32} - 1)$.
<m> ~ <n></n></m>	Any number between 'm' and 'n'.
domain name[<n>]</n>	A string limited to a domain name shorter than 'n' characters (eg.
	www.ibm.com).
email address [<n>]</n>	A string limited to an email address shorter than `n' characters (eg.
	joe@www.ibm.com).
ip address	A string limited to an IP address (eg. 192.168.1.1).
mac address	A string limited to contain a MAC address without hyphens or colons.
boolean	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or
	Disable].
<value1>,</value1>	Enumeration. Only given values are valid.
<value2>,</value2>	
<value3>,</value3>	
blank	A blank string.

everything inside <>	A description
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique
	integer by the server.
text	SQLite data type. The value is a text string, stored using the database
encoding (UTF-8, UTF-16BE or UTF-16-LE).	
coordinate	x, y coordinate (eg. 0,0)
window size	window width and height (eg. 800x600)

NOTE: The camera should not be restarted when parameters are changed.

7.1 system

Group: system

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
hostname	string[64]	Mega-Pixel	1/6	Host name of server
		Network		(Network Camera,
		Camera		Wireless Network Camera,
				Video Server,
				Wireless Video Server).
ledoff	<boolean></boolean>	0	6/6	Turn on (0) or turn off (1) all
				led indicators.
lowlight	<boolean></boolean>	1	6/6	Turn on white light LED under
				all conditions.
				Only turn on white light LED in
				low light conditions.
				(product dependent)
date	<yyyy <="" mm="" td=""><td><current< td=""><td>6/6</td><td>Current date of system. Set to</td></current<></td></yyyy>	<current< td=""><td>6/6</td><td>Current date of system. Set to</td></current<>	6/6	Current date of system. Set to
	DD>,	date>		'keep' to keep date
	keep,			unchanged. Set to 'auto' to
	auto			use NTP to synchronize date.
time	<hh:mm:s< td=""><td><current< td=""><td>6/6</td><td>Current time of the system.</td></current<></td></hh:mm:s<>	<current< td=""><td>6/6</td><td>Current time of the system.</td></current<>	6/6	Current time of the system.
	s>,	time>		Set to 'keep' to keep time
	keep,			unchanged. Set to 'auto' to
	auto			use NTP to synchronize time.
datetime	<mmddhh< td=""><td><blank></blank></td><td>6/6</td><td>Another current time format</td></mmddhh<>	<blank></blank>	6/6	Another current time format
	mmYYYY.ss			of the system.
	>			

ntp	<domain< th=""><th><blank></blank></th><th>6/6</th><th>NTP server.</th></domain<>	<blank></blank>	6/6	NTP server.
	name>,			*Do not use "skip to invoke
	<ip< td=""><td></td><td></td><td>default server" for default</td></ip<>			default server" for default
	address>,			value.
	<blank></blank>			
timezoneindex	-489 ~ 529	320	6/6	Indicate timezone and area.
			,	-480: GMT-12:00 Eniwetok,
				, Kwajalein
				-440: GMT-11:00 Midway
				Island, Samoa
				-400: GMT-10:00 Hawaii
				-360: GMT-09:00 Alaska
				-320: GMT-08:00 Las Vegas,
				San_Francisco,
				Vancouver
				-280: GMT-07:00 Mountain
				Time, Denver
				-281: GMT-07:00 Arizona
				-240: GMT-06:00 Central
				America, Central Time,
				Mexico City, Saskatchewan
				-200: GMT-05:00 Eastern
				Time, New York, Toronto
				-201: GMT-05:00 Bogota,
				Lima, Quito, Indiana
				-180: GMT-04:30 Caracas
				-160: GMT-04:00 Atlantic
				Time, Canada, La Paz,
				Santiago
				-140: GMT-03:30
				Newfoundland
				-120: GMT-03:00 Brasilia,
				Buenos Aires,
				Georgetown, Greenland
				-80: GMT-02:00 Mid-Atlantic
				-40: GMT-01:00 Azores,
				Cape_Verde_IS.
				0: GMT Casablanca,
				Greenwich Mean Time:
				Dublin,

Edinburgh, Lisbon, Lon	
40: GMT 01:00 Amster	lam,
Berlin, Rome, Stockholn	n,
Vienna, Madrid, Paris	
41: GMT 01:00 Warsaw	,
Budapest, Bern	
80: GMT 02:00 Athens,	
Helsinki, Istanbul, Riga	
81: GMT 02:00 Cairo	
82: GMT 02:00 Lebanor	٦,
Minsk	
83: GMT 02:00 Israel	
120: GMT 03:00 Baghda	ad,
Kuwait, Riyadh, Moscow	ı, St.
Petersburg, Nairobi	
121: GMT 03:00 Iraq	
140: GMT 03:30 Tehran	I
160: GMT 04:00 Abu Dł	habi,
Muscat, Baku,	
Tbilisi, Yerevan	
180: GMT 04:30 Kabul	
200: GMT 05:00	
Ekaterinburg, Islamaba	d,
Karachi, Tashkent	
220: GMT 05:30 Calcutt	ta,
Chennai, Mumbai, New	Delhi
230: GMT 05:45 Kathm	andu
240: GMT 06:00 Almaty	1,
Novosibirsk, Astana, Dh	iaka,
Sri Jayawardenepura	
260: GMT 06:30 Rango	on
280: GMT 07:00 Bangko	
Hanoi, Jakarta, Krasnoy	
320: GMT 08:00 Beijing	
Chongging, Hong Kong,	
Lumpur, Singapore, Taip	
360: GMT 09:00 Osaka,	
Sapporo, Tokyo, Seoul,	
Yakutsk	
380: GMT 09:30 Adelaid	

			1	1
				Darwin
				400: GMT 10:00 Brisbane,
				Canberra, Melbourne,
				Sydney, Guam, Vladivostok
				440: GMT 11:00 Magadan,
				Solomon Is., New Caledonia
				480: GMT 12:00 Aucklan,
				Wellington, Fiji, Kamchatka,
				Marshall Is.
				520: GMT 13:00 Nuku'Alofa
daylight_enable	<boolean></boolean>	0	6/6	Enable automatic daylight
				saving time in time zone.
daylight_dstactualmode	<boolean></boolean>	1	6/7	Check if current time is under
				daylight saving time.
				(Used internally)
daylight_auto_begintime	string[19]	NONE	6/7	Display the current daylight
				saving start time.
daylight_auto_endtime	string[19]	NONE	6/7	Display the current daylight
				saving end time.
daylight_timezones	string	,-360,-320,	6/6	List time zone index which
		-280,-240,		support daylight saving time.
		-241,-200,		
		-201,-160,		
		-140,-120,		
		-80,-40,0,		
		40,41,80,		
		81,82,83,		
		120,140,		
		380,400,48		
		0		
updateinterval	0,	0	6/6	0 to Disable automatic time
	3600,			adjustment, otherwise, it
	86400,			indicates the seconds
	604800,			between NTP automatic
	2592000			update intervals.
restore	0,	N/A	7/6	Restore the system
	<positive< td=""><td></td><td></td><td>parameters to default values</td></positive<>			parameters to default values
	integer>			after <value> seconds.</value>
reset	0,	N/A	7/6	Restart the server after
	<positive< td=""><td></td><td></td><td><value> seconds if <value></value></value></td></positive<>			<value> seconds if <value></value></value>
	-posicive			

	integer>			is non-negative.
restoreexceptnet	<any< td=""><td>N/A</td><td>7/6</td><td>Restore the system</td></any<>	N/A	7/6	Restore the system
	value>			parameters to default values
				except (ipaddress, subnet,
				router, dns1, dns2, pppoe).
				This command can cooperate
				with other
				"restoreexceptXYZ"
				commands. When
				cooperating with others, the
				system parameters will be
				restored to the default value
				except for a union of the
				combined results.
restoreexceptdst	<any< td=""><td>N/A</td><td>7/6</td><td>Restore the system</td></any<>	N/A	7/6	Restore the system
	value>			parameters to default values
				except all daylight saving time
				settings.
				This command can cooperate
				with other
				"restoreexceptXYZ"
				commands. When
				cooperating with others, the
				system parameters will be
				restored to default values
				except for a union of
				combined results.
restoreexceptlang	<any< td=""><td>N/A</td><td>7/6</td><td>Restore the system</td></any<>	N/A	7/6	Restore the system
	Value>			parameters to default values
				except the custom language
				file the user has uploaded.
				This command can cooperate
				with other
				"restoreexceptXYZ"
				commands. When
				cooperating with others, the
				system parameters will be
				restored to the default value
				except for a union of the
				combined results.

restoreexceptvadp	<integer></integer>	N/A	99/6	Restore the system
				parameters to default values
				except the vadp parameters
				and VADP modules that stored
				in the system.
				This command can cooperate
				with other
				"restoreexceptXYZ"
				commands. When
				cooperating with others, the
				system parameters will be
				restored to the default value
				except for a union of the
				combined results.

7.1.1 system.info

Subgroup of **system**: **info** (The fields in this group are unchangeable.)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
modelname	string[40]	FE8171	0/7	Internal model name of the
				server (eg. IP7139)
extendedmodelname	string[40]	FE8171	0/7	ODM specific model name of
				server (eg. DCS-5610). If it
				is not an ODM model, this
				field will be equal to
				"modelname"
serialnumber	<mac< td=""><td><product< td=""><td>0/7</td><td>12 characters MAC address</td></product<></td></mac<>	<product< td=""><td>0/7</td><td>12 characters MAC address</td></product<>	0/7	12 characters MAC address
	address>	mac		(without hyphens).
		address>		
firmwareversion	string[40]	<product< td=""><td>0/7</td><td>Firmware version, including</td></product<>	0/7	Firmware version, including
		dependent		model, company, and
		>		version number in the
				format:
				<model-brand-version></model-brand-version>
language_count	<integer></integer>	9	0/7	Number of webpage
				languages available on the
				server.
language_i<0~(count-1)>	string[16]	<product< td=""><td>0/7</td><td>Available language lists.</td></product<>	0/7	Available language lists.
		dependent		

		>		
customlanguage_maxcoun	<integer></integer>	1	0/6	Maximum number of custom
t				languages supported on the
				server.
customlanguage_count	<integer></integer>	0	0/6	Number of custom
				languages which have been
				uploaded to the server.
customlanguage_i<0~(ma	string	<blank></blank>	0/6	Custom language name.
xcount-1)>				

7.2 status

Group: status

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
videoactualmodulation	ntsc,	1	4/7	The actual modulation
<product dependent=""></product>	pal			type
				(videoin.type=0).
di_i<0~(ndi-1)>	<boolean></boolean>	0	1/7	0 => Inactive, normal
<product dependent=""></product>				1 => Active, triggered
				(capability.ndi > 0)
do_i<0~(ndo-1)>	<boolean></boolean>	0	1/7	0 => Inactive, normal
<product dependent=""></product>				1 => Active, triggered
				(capability.ndo > 0)
daynight	day, night	<product< td=""><td>7/7</td><td>Current status of day,</td></product<>	7/7	Current status of day,
<product dependent=""></product>		dependent>		night.
onlinenum_rtsp	integer	0	6/7	Current number of RTSP
				connections.
onlinenum_httppush	integer	0	6/7	Current number of HTTP
				push server
				connections.
eth_i0	<string></string>	<product< td=""><td>1/7</td><td>Get network information</td></product<>	1/7	Get network information
		dependent>		from mii-tool.
vi_i<0~(nvi-1)>	<boolean></boolean>	0	1/7	Virtual input
<product dependent=""></product>				0 => Inactive
				1 => Active
				(capability.nvi > 0)

7.3 digital input behavior define

Group: **di_i<0~(ndi-1)> (**capability.ndi > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
normalstate	high,	high	1/1	Indicates open circuit or
	low			closed circuit (inactive
				status)

7.4 digital output behavior define

Group: **do_i<0~(ndo-1)> (**capability.ndo > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
normalstate	open,	open	1/1	Indicate open circuit or
	grounded			closed circuit (inactive
				status)

7.5 security

Group: security

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
privilege_do	view, operator,	operator	6/6	Indicate which privileges
<product dependent=""></product>	admin			and above can control
				digital output
				(capability.ndo > 0)
privilege_camctrl	view, operator,	view	6/6	Indicate which privileges
<product dependent=""></product>	admin			and above can control PTZ
				(capability.ptzenabled > 0
				or capability.eptz > 0)
user_i0_name	string[64]	root	6/7	User name of root
user_i<1~20>_name	string[64]	<blank></blank>	6/7	User name
user_i0_pass	password[64]	<blank></blank>	6/6	Root password
user_i<1~20>_pass	password[64]	<blank></blank>	7/6	User password
user_i0_privilege	viewer,	admin	6/7	Root privilege
	operator,			
	admin			
user_i<1~20>_ privilege	viewer,	<blank></blank>	6/6	User privilege

	operator,		
	admin		

7.6 network

Group: network

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
preproces	<positive integer></positive 	 blank>	7/6	An 32-bit integer, each bit can be set separately as follows: Bit 0 => HTTP service; Bit 1=> HTTPS service; Bit 2=> FTP service; Bit 3 => Two way audio and RTSP Streaming service; To stop service before changing its port settings. It's recommended to set this parameter when change a service port to the port occupied by another service currently. Otherwise, the service may fail. Stopped service will auto-start after changing port settings. Ex: Change HTTP port from 80 to 5556, and change RTP port for video from 5556 to 20480. Then, set preprocess=9 to stop both service first. "/cgi-bin/admin/setparam.cgi? network_preprocess=9&network_http_port=555 6& network_rtp_videoport=20480"
type	lan, pppoe <product dependent></product 	lan	6/6	Network connection type.
resetip	<boolean></boolean>	1	6/6	 1 => Get ipaddress, subnet, router, dns1, dns2 from DHCP server at next reboot. 0 => Use preset ipaddress, subnet, rounter, dns1, and dns2.
ipaddress	<ip address></ip 	<product dependent></product 	6/6	IP address of server.

subnet	<ip< th=""><th><blank></blank></th><th>6/6</th><th>Subnet mask.</th></ip<>	<blank></blank>	6/6	Subnet mask.
	address>			
router	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Default gateway.</td></ip<>	<blank></blank>	6/6	Default gateway.
	address>			
dns1	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Primary DNS server.</td></ip<>	<blank></blank>	6/6	Primary DNS server.
	address>			
dns2	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Secondary DNS server.</td></ip<>	<blank></blank>	6/6	Secondary DNS server.
	address>			
wins1	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Primary WINS server.</td></ip<>	<blank></blank>	6/6	Primary WINS server.
	address>			
wins2	<ip< td=""><td><blank></blank></td><td>6/6</td><td>Secondary WINS server.</td></ip<>	<blank></blank>	6/6	Secondary WINS server.
	address>			

7.6.1 802.1x

Subgroup of **network: ieee8021x** (capability.protocol.ieee8021x > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap,	eap-peap	6/6	Selected EAP method
	eap-tls			
identity_peap	String[64]	<blank></blank>	6/6	PEAP identity
identity_tls	String[64]	<blank></blank>	6/6	TLS identity
password	String[254]	<blank></blank>	6/6	Password for TLS
privatekeypassword	String[254]	<blank></blank>	6/6	Password for PEAP
ca_exist	<boolean></boolean>	0	6/6	CA installed flag
ca_time	<integer></integer>	0	6/7	CA installed time.
				Represented in EPOCH
ca_size	<integer></integer>	0	6/7	CA file size (in bytes)
certificate_exist	<boolean></boolean>	0	6/6	Certificate installed flag (for
				TLS)
certificate_time	<integer></integer>	0	6/7	Certificate installed time.
				Represented in EPOCH
certificate_size	<integer></integer>	0	6/7	Certificate file size (in bytes)
privatekey_exist	<boolean></boolean>	0	6/6	Private key installed flag (for
				TLS)
privatekey_time	<integer></integer>	0	6/7	Private key installed time.
				Represented in EPOCH
privatekey_size	<integer></integer>	0	6/7	Private key file size (in bytes)

7.6.2 QOS

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable/disable CoS (IEEE 802.1p)
vlanid	1~4095	1	6/6	VLAN ID
video	0~7	0	6/6	Video channel for CoS
audio	0~7	0	6/6	Audio channel for CoS
<product< td=""><td></td><td></td><td></td><td>(capability.naudio > 0)</td></product<>				(capability.naudio > 0)
dependent>				
eventalarm	0~7	0	6/6	Event/alarm channel for CoS
management	0~7	0	6/6	Management channel for CoS
eventtunnel	0~7	0	6/6	Event/Control channel for CoS

Subgroup of **network: qos_cos** (capability.protocol.qos.cos > 0)

Subgroup of **network: qos_dscp** (capability.protocol.qos.dscp > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable/disable DSCP
video	0~63	0	6/6	Video channel for DSCP
audio	0~63	0	6/6	Audio channel for DSCP
				(capability.naudio > 0)
eventalarm	0~63	0	6/6	Event/alarm channel for DSCP
management	0~63	0	6/6	Management channel for DSCP
eventtunnel	0~63	0	6/6	Event/Control channel for DSCP

7.6.3 IPV6

Subgroup of **network**: **ipv6** (capability.protocol.ipv6 > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable IPv6.
addonipaddress	<ip address=""></ip>	<blank></blank>	6/6	IPv6 IP address.
addonprefixlen	0~128	64	6/6	IPv6 prefix length.
addonrouter	<ip address=""></ip>	<blank></blank>	6/6	IPv6 router address.
addondns	<ip address=""></ip>	<blank></blank>	6/6	IPv6 DNS address.
allowoptional	<boolean></boolean>	0	6/6	Allow manually setup of IP
				address setting.

7.6.4 FTP

Subgroup of **network**: **ftp**

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
port	21, 1025~65535	21	6/6	Local ftp server port.

7.6.5 HTTP

Subgroup of **network**: http

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	80	1/6	HTTP port.
alternateport	1025~65535	8080	6/6	Alternate HTTP port.
authmode	basic, digest	basic	1/6	HTTP authentication mode.
s0_accessname	string[32]	video.mjpg	1/6	<pre>HTTP server push access name for stream 1. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 0)</pre>
s1_accessname <product dependent></product 	string[32]	video2.mjpg	1/6	HTTP server push access name for stream 2. (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 1)
s2_accessname <product dependent></product 	string[32]	video3.mjpg	1/6	Http server push access name for stream 3 (capability.protocol.spush_mjpeg =1 and capability.nmediastream > 2)
anonymousviewing	<boolean></boolean>	0	1/6	Enable anoymous streaming viewing.

7.6.6 HTTPS port

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
port	443, 1025 ~	443	1/6	HTTPS port.
	65535			

Subgroup of **network**: **https_port** (capability.protocol.https > 0)

7.6.7 RTSP

Subgroup of **network**: **rtsp** (capability.protocol.rtsp > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~	554	1/6	RTSP port.
	65535			(capability.protocol.rtsp=1)
anonymousviewing	<boolean></boolean>	0	1/6	Enable anoymous streaming
				viewing.
authmode	disable,	disable	1/6	RTSP authentication mode.
	basic,			(capability.protocol.rtsp=1)
	digest			
s0_accessname	<boolean></boolean>	live.sdp	1/6	RTSP access name for
				stream1.
				(capability.protocol.rtsp=1
				and capability.nmediastream
				> 0)
s1_accessname	<boolean></boolean>	live2.sdp	1/6	RTSP access name for
				stream2.
				(capability.protocol.rtsp=1
				and capability.nmediastream
				> 1)
s2_accessname	<boolean></boolean>	live3.sdp	1/6	RTSP access name for
				stream3
				(capability.protocol.rtsp=1
				and capability.nmediastream
				> 2)

7.6.7.1 RTSP multicast

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
alwaysmulticast	<boolean></boolean>	0	4/4	Enable always multicast.
ipaddress	<ip address=""></ip>	For n=0, 239.128.1.99 For n=1, 239.128.1.100, and so on.	4/4	Multicast IP address.
videoport	1025 ~ 65535	5560+n*2	4/4	Multicast video port.
audioport <product dependent></product 	1025 ~ 65535	5562+n*2	4/4	Multicast audio port. (capability.naudio > 0)
ttl	1 ~ 255	15	4/4	Mutlicast time to live value.

Subgroup of **network_rtsp_s<0~(n-1)>**: **multicast**, n is stream count (capability.protocol.rtp.multicast > 0)

7.6.8 SIP port

Subgroup of **network**: **sip** (capability.protocol.sip> 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
port	1025 ~ 65535	5060	1/6	SIP port.

7.6.9 RTP port

Subgroup of network: rtp

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
videoport	1025 ~ 65535	5556	6/6	Video channel port for RTP.
				(capability.protocol.rtp_unicast=1)
audioport	1025 ~ 65535	5558	6/6	Audio channel port for RTP.
				(capability.protocol.rtp_unicast=1)

7.6.10 PPPoE

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
user	string[128]	<blank></blank>	6/6	PPPoE account user name.
pass	password[64]	<blank></blank>	6/6	PPPoE account password.

Subgroup of **network**: **pppoe** (capability.protocol.pppoe > 0)

7.7 IP Filter

Group: ipfilter

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean></boolean>	0	6/6	Enable access list filtering.
admin_enable	<boolean></boolean>	0	6/6	Enable administrator IP address.
admin_ip	String[44]	<blank></blank>	6/6	Administrator IP address.
maxconnection	1~10	10	6/6	Maximum number of concurrent streaming connection(s).
type	0, 1	1	6/6	Ipfilter policy : 0 => allow 1 => deny
ipv4list_i<0~9>	Single address: <ip address=""> Network address: <ip <br="" address="">network mask> Range address:<start ip<br="">address - end ip address></start></ip></ip>	<blank></blank>	6/6	IPv4 address list.
ipv6list_i<0~9>	String[44]	<blank></blank>	6/6	IPv6 address list.

7.8 Video input

Group: videoin

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
cmosfreq	50, 60	60	4/4	CMOS frequency.
				(capability.videoin.type=2)
whitebalance	auto, manual	auto	4/4	"auto" indicates auto white
				balance.
				"manual" indicates keep current
				value.
exposurelevel	0~12	6	4/4	Exposure level
enableblc	<boolean></boolean>	0	4/4	Enable backlight compensation.
color	0,1	1	4/4	0 =>monochrome
				1 => color
flip	<boolean></boolean>	0	4/4	Flip the image.
mirror	<boolean></boolean>	0	4/4	Mirror the image.
ptzstatus	<integer></integer>	2	1/7	A 32-bit integer, each bit can be
				set separately as follows:
				Bit 0 => Support camera control
				function; 0(not support),
				1(support)
				Bit 1 => Built-in or external
				camera; 0 (external), 1(built-in)
				Bit 2 => Support pan operation;
				0(not support), 1(support)
				Bit 3 => Support tilt operation;
				0(not support), 1(support)
				Bit 4 => Support zoom
				operation; 0(not support),
				1(support)
				Bit 5 => Support focus
				operation; 0(not support),
				1(support)
text	string[16]	<blank></blank>	1/4	Enclose caption.
textonvideo_position	top, bottom	top	4/4	Position of timestamp and video
				title on image

textonvideo_size	15,25,30	15	4/4	Timestamp and video title font-size
maxexposure	1, 15, 30, 60, 120, 240, 480 <product dependent></product 	30	4/4	Maximum exposure time.
options	framerate	framerate	4/4	Video input option: (1) video frame rate first mode
enablepreview	<boolean></boolean>	0	1/4	Usage for UI of exposure settings. Preview settings of video profile.

7.8.1 Video input setting per channel

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
	50.00	60	(get/set)	
cmosfreq	50, 60	60	4/4	CMOS frequency.
				(capability.videoin.type=2)
whitebalance	auto, manual	auto	4/4	"auto" indicates auto white
				balance.
				"manual" indicates keep
				current value.
rgain	0~100	30	4/4	Manual set rgain value of
				gain control setting.
bgain	0~100	30	4/4	Manual set bgain value of
				gain control setting.
exposurelevel	0~12	6	4/4	Exposure level
enableblc	0~1	0	4/4	Enable backlight
				compensation
agcmode	auto,fixed	1	4/4	Set auto gain control mode.
maxgain	0~100	100	4/4	Manual set maximum gain
				value.
mingain	0~100	0	4/4	Manual set minimum gain
				value.
color	0, 1	1	4/4	0 =>monochrome
				1 => color
flip	<boolean></boolean>	0	4/4	Flip the image.

mirror	<boolean></boolean>	0	4/4	Mirror the image.
ptzstatus	<integer></integer>	2	1/7	A 32-bit integer, each bit can
				be set separately as follows:
				Bit 0 => Support camera
				control function; 0(not
				support), 1(support)
				Bit 1 => Built-in or
				external camera; 0
				(external), 1(built-in)
				Bit 2 => Support pan
				operation; 0(not support),
				1(support)
				Bit 3 => Support tilt
				operation; 0(not support),
				1(support)
				Bit 4 => Support zoom
				operation; 0(not support),
				1(support)
				Bit 5 => Support focus
				operation; 0(not support),
				1(support)
text	string[60]	<blank></blank>	1/4	Enclose caption.
imprinttimestamp	<boolean></boolean>	0	4/4	Overlay time stamp on
				video.
exposuremode	auto,fixed	auto	4/4	Exposure mode
flickerless	<boolean></boolean>	0	4/4	Avoid flickering on images.
minexposure	1~32000	32000	4/4	Minimum exposure time.
maxexposure	1~32000	30	4/4	Maximum exposure time.
options	crop	crop	4/4	Video input option: cropping
				mode
 crop_size	<window size=""></window>	1952x1944	1/4	Crop width and height.
	(WxH)			(1)1952x1944
				(2)1920x1080
enablepreview	<boolean></boolean>	0	1/4	Usage for UI of exposure
				settings. Preview settings of
				video profile.
s<0~(m-1)>_codectype	mpeg4, mjpeg,	H264	1/4	Video codec type.
	h264			
s<0~(m-1)>_resolution	Reference	1536x1536	1/4	Video resolution in pixels.
-	capability_vide			

	oin_resolution			
s<0~(m-1)>_mpeg4_intrap	250, 500,	1000	4/4	Intra frame period in
eriod	1000, 2000,			milliseconds.
	3000, 4000			
s<0~(m-1)>_mpeg4_bitrate	average,	average	4/4	"average" indicates the
restriction	upperbound			average bit rate will be equal
				to its target bit rate.
				"upperbound" indicates the
				bit rate will always not
				exceed its target bit rate.
s<0~(m-1)>_mpeg4_priorit	framerate,	framerate	4/4	The policy to apply when the
ypolicy	imagequality			target bit rate is not
				sufficient to satisfy current
				encoded conditions.
				"framerate" indicates frame
				rate first.
				"imagequality" indicates
				image quality first.
s<0~(m-1)>_mpeg4_rateco	cbr, vbr	vbr	4/4	cbr, constant bitrate
ntrolmode				vbr, fix quality
s<0~(m-1)>_mpeg4_quant	1~5	3	4/4	Quality of video when
	99, 100			choosing vbr in
				"ratecontrolmode".
				99 is the customized manual
				input setting.
				1 = worst quality, 5 = best
				quality.
	2.24			100 is percentage mode.
s<0~(m-1)>_mpeg4_qvalue	2~31	7	4/4	Manual video quality level
				input.
				(s<0~(m-1)>_mpeg4_quan
c < 0 = (m - 1) > m - c < 4 = - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c < - c	1~100	29	4/4	t = 99)
s<0~(m-1)>_mpeg4_qperce	1~100	23	4/4	Manual video quality level
nt				input. (s<0~(m-1)>_mpeg4_quan
				t = 100
s<0~(m-1)>_mpeg4_bitrate	1000~160000	3000000	4/4	Set bit rate in bps when
	00	500000		choosing cbr in
	<product< td=""><td></td><td></td><td>"ratecontrolmode".</td></product<>			"ratecontrolmode".
	dependent>			
L			I	I

s<0~(m-1)>_mpeg4_maxfr	1~15	15	1/4	Set maximum frame rate in
ame				fps (for MPEG-4).
s<0~(m-1)>_h264_intraperi od	250, 500, 1000, 2000, 3000, 4000	1000	4/4	Intra frame period in milliseconds.
s<0~(m-1)>_h264_bitratere striction	average, upperbound	average	4/4	"average" indicates the average bit rate will be equal to its target bit rate. "upperbound" indicates the bit rate will always not exceed its target bit rate.
s<0~(m-1)>_h264_priorityp olicy	framerate, imagequality	framerate	4/4	The policy to apply when the target bit rate is not sufficient to satisfy current encoded conditions. "framerate" indicates frame rate first. "imagequality" indicates image quality first.
s<0~(m-1)>_h264_ratecont rolmode	cbr, vbr	vbr	4/4	cbr, constant bitrate vbr, fix quality
s<0~(m-1)>_h264_quant	1~5 99, 100	3	4/4	Quality of video when choosing vbr in "ratecontrolmode". 99 is the customized manual input setting. 1 = worst quality, 5 = best quality. 100 is percentage mode.
s<0~(m-1)>_h264_qvalue	0~51	2	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 99)
s<0~(m-1)>_h264_qpercen t	1~100	44	4/4	Manual video quality level input. (s<0~(m-1)>_h264_quant = 100)
s<0~(m-1)>_h264_bitrate	1000~160000 00	3000000	4/4	Set bit rate in bps when choosing cbr in "ratecontrolmode".

s<0~(m-1)>_h264_maxfra	1~15	15	1/4	Set maximum frame rate in
me			-, .	fps (for h264).
s<0~(m-1)>_h264_profile	0~2	1	1/4	Indicate H264 profiles
<pre><pre>content</pre></pre>		-	-/ '	0: baseline
				1: main profile
				2: high profile
s<0~(m-1)>_mjpeg_bitrater	2007200	average	4/4	"average" indicates the
estriction	average,	average	4/4	_
estriction	upperbound			average bit rate will be equal
				to its target bit rate.
				"upperbound" indicates the
				bit rate will always not
				exceed its target bit rate.
s<0~(m-1)>_mjpeg_priority	framerate,	framerate	4/4	The policy to apply when the
policy	imagequality			target bit rate is not
				sufficient to satisfy current
				encoded conditions.
				"framerate" indicates frame
				rate first.
				"imagequality" indicates
				image quality first.
s<0~(m-1)>_mjpeg_ratecon	cbr, vbr	vbr	4/4	cbr, constant bitrate
trolmode				vbr, fix quality
s<0~(m-1)>_mjpeg_quant	1~5	3	4/4	Quality of JPEG video.
	99, 100			99 is the customized manual
				input setting.
				1 = worst quality, 5 = best
				quality.
				100 is percentage mode.
s<0~(m-1)>_mjpeg_qvalue	2~97	50	4/4	Manual video quality level
				input.
				(s<0~(m-1)>_mjpeg_quan
				t = 99)
s<0~(m-1)>_mjpeg_qperce	1~100	49	4/4	Manual video quality level
nt				input.
				(s<0~(m-1)>_mjpeg_quan
				t = 100)
s<0~(m-1)>_mjpeg_maxfra	1~15	15	1/4	Set maximum frame rate in
me				fps (for JPEG).
s<0~(m-1)>_mjpeg_bitrate	1000~160000	30000000	4/4	Set bit rate in bps when
	00			choosing cbr in

				"ratecontrolmode".
s<0~(m-1)>_forcei	1	N/A	7/6	Force I frame.
s<0~(m-1)>_fisheyede	10, 1P, 2P,	10	1/4	Local dewarp mode.
warpmode	1R, 4R for			"10" is original mode
	ceiling/floor			(disable).
	mount			
	10, 1P, 1R,			
	4R for wall			
	mount			
wdrc_mode	0~2	0	4/4	WDR enhanced.
				0: off
				1: Sensitivity low
				2: Sensitivity high
wdrc_strength	0~2	1	4/4	WDR enhanced.
				0: low
				1: medium
				2: high
mounttype	ceiling, wall,	wall	1/6	Mount type
	floor			
enableimgreport	0, 1	0	1/6	Image report
enablewatermark	0, 1	0	1/6	Watermark

7.8.1.1 Alternative video input profiles per channel

In addition to the primary setting of video input, there can be alternative profile video input setting for each channel which might be for different scene of light (daytime or nighttime).

Group: videoin_c0_profile_i<0~(m-1)> (capability. nvideoinprofile > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
			(gel/sel)	
enable	<boolean></boolean>	0	4/4	Enable/disable this profile setting
policy	day,	night	4/4	The mode which the profile is
	night,			applied to.
	schedule			
begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
endtime	hh:mm	06:00	4/4	End time of schedule mode.
exposuremode	auto,fixed	auto	4/4	Exposure Mode
flickerless	<boolean></boolean>	0	4/4	Avoid flickering on images.
minexposure	1~32000	32000	4/4	Minimum exposure time.

maxexposure1~32000304/4Maximum exposure time.enableblc <boolean>04/4Enable backlight compensation.exposurelevel0~1264/4Exposure levelagcmodeauto,fixedauto4/4Set auto gain control mode.maxgain0~10004/4Manual set maximum gain value.whitebalanceauto, manualauto4/4Manual set minimum gain value.rgain0~10004/4Manual set minimum gain value.rgain0~100304/4Manual set rgain value of gain control setting.pain0~100304/4Manual set rgain value of gain control setting.bgain0~100304/4Manual set logain value of gain control setting.wdrc_mode0~204/4WDR enhanced.wdrc_strength0~214/4WDR enhanced.wdrc_strength0~214/4UDR enhanced.iiiiiiwdrc_strength0~21ii<t< th=""><th></th><th></th><th></th><th></th><th></th></t<></boolean>					
exposurelevel $0 \sim 12$ 6 $4/4$ Exposure levelagcmodeauto,fixedauto $4/4$ Set auto gain control mode.maxgain $0 \sim 100$ 100 $4/4$ Manual set maximum gain value.mingain $0 \sim 100$ 0 $4/4$ Manual set minimum gain value.whitebalanceauto, manualauto $4/4$ "auto" indicates auto white balance. "manual" indicates keep current value.rgain $0 \sim 100$ 30 $4/4$ Manual set rgain value of gain control setting.bgain $0 \sim 100$ 30 $4/4$ Manual set bgain value of gain control setting.wdrc_mode $0 \sim 2$ 0 $4/4$ WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity highwdrc_strength $0 \sim 2$ 1 $4/4$ WDR enhanced. 0: low 1: medium	maxexposure	1~32000	30	4/4	Maximum exposure time.
agcmodeauto,fixedauto4/4Set auto gain control mode.maxgain0~1001004/4Manual set maximum gain value.mingain0~10004/4Manual set minimum gain value.whitebalanceauto, manualauto4/4*auto" indicates auto white balance. *manual" indicates keep current value.rgain0~100304/4Manual set rgain value of gain control setting.bgain0~100304/4Manual set bgain value of gain control setting.wdrc_mode0~204/4WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity highwdrc_strength0~214/4WDR enhanced. 0: low 1: medium	enableblc	<boolean></boolean>	0	4/4	Enable backlight compensation.
maxgain0~1001004/4Manual set maximum gain value.mingain0~10004/4Manual set minimum gain value.whitebalanceauto, manualauto4/4"auto" indicates auto white balance. "manual" indicates keep current value.rgain0~100304/4Manual set rgain value of gain control setting.bgain0~100304/4Manual set bgain value of gain control setting.wdrc_mode0~204/4WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity highwdrc_strength0~214/4WDR enhanced. 0: low 1: medium	exposurelevel	0~12	6	4/4	Exposure level
mingain0~10004/4Manual set minimum gain value.whitebalanceauto, manualauto4/4"auto" indicates auto white balance. "manual" indicates keep current value.rgain0~100304/4Manual set rgain value of gain control setting.bgain0~100304/4Manual set bgain value of gain control setting.wdrc_mode0~204/4Manual set bgain value of gain control setting.wdrc_strength0~214/4WDR enhanced. 0: low 1: medium	agcmode	auto,fixed	auto	4/4	Set auto gain control mode.
whitebalanceauto, manualauto4/4"auto" indicates auto white balance. "manual" indicates keep current value.rgain0~100304/4Manual set rgain value of gain control setting.bgain0~100304/4Manual set bgain value of gain control setting.wdrc_mode0~204/4WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity highwdrc_strength0~214/4WDR enhanced. 0: low 1: medium	maxgain	0~100	100	4/4	Manual set maximum gain value.
NoteNo	mingain	0~100	0	4/4	Manual set minimum gain value.
wdrc_strength0~214/4"manual" indicates keep current value."manual" indicates keep current value."manual" indicates keep current value.Manual set rgain value of gain control setting.Manual set bgain value of gain control setting.	whitebalance	auto, manual	auto	4/4	"auto" indicates auto white
Image: space s					balance.
rgain0~100304/4Manual set rgain value of gain control setting.bgain0~100304/4Manual set bgain value of gain control setting.wdrc_mode0~204/4WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity highwdrc_strength0~214/4WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity high					"manual" indicates keep current
bgain0~100304/4Manual set bgain value of gain control setting.wdrc_mode0~204/4WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity highwdrc_strength0~214/4WDR enhanced. 0: off 1: Sensitivity high					value.
bgain0~100304/4Manual set bgain value of gain control setting.wdrc_mode0~204/4WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity highwdrc_strength0~214/4WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity high	rgain	0~100	30	4/4	Manual set rgain value of gain
wdrc_mode 0~2 0 4/4 WDR enhanced. wdrc_strength 0~2 1 4/4 0: off wdrc_strength 0~2 1 4/4 WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity high wdrc_strength 0~2 1 4/4 WDR enhanced. 0: low 1: medium					control setting.
wdrc_mode 0~2 0 4/4 WDR enhanced. 0: off 1: Sensitivity low 1: Sensitivity low wdrc_strength 0~2 1 4/4 WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity high wdrc_strength 0~2 1 4/4 WDR enhanced. 0: low 1: medium	bgain	0~100	30	4/4	Manual set bgain value of gain
wdrc_strength 0~2 1 4/4 WDR enhanced. 0: off 1: Sensitivity low 2: Sensitivity high 1 4/4 WDR enhanced. 0: low 1: medium 1: medium					control setting.
wdrc_strength 0~2 1 4/4 WDR enhanced. 0: low 1: medium	wdrc_mode	0~2	0	4/4	WDR enhanced.
wdrc_strength 0~2 1 4/4 WDR enhanced. 0: low 1: medium					0: off
wdrc_strength 0~2 1 4/4 WDR enhanced. 0: low 1: medium					1: Sensitivity low
0: low 1: medium					2: Sensitivity high
1: medium	wdrc_strength	0~2	1	4/4	WDR enhanced.
					0: low
2: high					1: medium
					2: high

7.9 Video input preview

The temporary settings for video preview

Group: videoinpreview

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
exposuremode	auto,fixed	auto	4/4	Exposure Mode
minexposure	1~32000	32000	4/4	Minimum exposure time.
maxexposure	1~32000	30	4/4	Maximum exposure time.
exposurelevel	0~12	6	4/4	Exposure level
enableblc	<boolean></boolean>	0	4/4	Enable backlight compensation.
wdrc_mode	0~2	0	4/4	WDR enhanced.
				0: off
				1: Sensitivity low
				2: Sensitivity high
wdrc_strength	0~2	1	4/4	WDR enhanced.

				0: low
				1: medium
				2: high
agcmode	auto,fixed	auto	4/4	Set auto gain control mode.
maxgain	0~100	100	4/4	Manual set maximum gain value.
mingain	0~100	0	4/4	Manual set minimum gain value.

7.10 IR cut control

Group: ircutcontrol	(capability.nvideoinprofile > 0)
---------------------	----------------------------------

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
mode	auto,	auto	6/6	Set IR cut control mode
	day,			
	night,			
	di,			
	schedule			
	<product< td=""><td></td><td></td><td></td></product<>			
	dependent>			
daymodebegintime	00:00~23:59	07:00	6/6	Day mode begin time
daymodeendtime	00:00~23:59	18:00	6/6	Day mod end time
bwmode	<boolean></boolean>	1	6/6	Switch to B/W in night mode if
				enabled
sensitivity	low,	normal	6/6	Sensitivity of light sensor
	normal,			
	high			
enableextled	<boolean></boolean>	0	1/6	External IR led enable

7.11 Image setting per channel

Group: image_c<0~(n-1)> for n channel products

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
brightness	-5~5	-5	4/4	Adjust brightness of image
				according to mode settings.
saturation	-5~5,100	0	4/4	Adjust saturation of image
				according to mode settings.
				100 for saturation percentage
				mode.

saturationpercent	0~100	50	4/4	Adjust saturation value of
				percentage when saturation=100
contrast	-5 ~ 5	0	4/4	Adjust contrast of image according
				to mode settings.
sharpness	-3~3,100	0	4/4	Adjust sharpness of image
				according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of
				percentage when sharpness=100
gammacurve	0~100	0	4/4	Gamma curve.
lowlightmode	<boolean></boolean>	1	4/4	Enable/disable low light mode.
profile_i0_enable	<boolean></boolean>	0	4/4	Enable/disable this profile setting
profile_i0_policy	day,	night	4/4	The mode which the profile is
	night,			applied to.
	schedule			
profile_i0_begintime	hh:mm	18:00	4/4	Begin time of schedule mode.
profile_i0_endtime	hh:mm	06:00	4/4	End time of schedule mode.
profile_i0_brightness	-5~5	-5	4/4	Adjust brightness of image
				according to mode settings.
profile_i0_saturation	-5~5,100	0	4/4	Adjust saturation of image
				according to mode settings.
				100 for saturation percentage
				mode.
profile_i0_saturationpercent	0~100	50	4/4	Adjust saturation value of
				percentage when saturation=100
profile_i0_contrast	-5 ~ 5	0	4/4	Adjust contrast of image according
				to mode settings.
profile_i0_sharpness	-3~3	0	4/4	Adjust sharpness of image
				according to mode settings.
profile_i0_sharpnesspercent	0~100	50	4/4	Adjust sharpness value of
				percentage when sharpness=100
profile_i0_gammacurve	0~100	0	4/4	Gamma curve
profile_i0_lowlightmode	<boolean></boolean>	1	4/4	Enable/disable low light mode.
profile_i0_wdrcstrength	0~2	1	4/4	WDR enhanced
				0: low
				1: medium
				2: high
profile_i0_wdrcmode	0~2	0	4/4	WDR enhanced
				0: off
				1: Sensitivity low

	2: Sensitivity high	
--	---------------------	--

7.12 Image setting for preview

Group: imagepreview_c<0~(n-1)> for n channel products

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
brightness	-5~5	-5	4/4	Adjust brightness of image
				according to mode settings.
saturation	-5~5,100	0	4/4	Adjust saturation of image
				according to mode settings.
				100 for saturation
				percentage mode.
saturationpercent	0~100	50	4/4	Adjust saturation value of
				percentage when
				saturation=100
contrast	-5 ~ 5	0	4/4	Adjust contrast of image
				according to mode settings.
sharpness	-3~3,100	0	4/4	Adjust sharpness of image
				according to mode settings.
sharpnesspercent	0~100	50	4/4	Adjust sharpness value of
				percentage when
				sharpness=100
gammacurve	0~100	0	4/4	Gamma curve
lowlightmode	<boolean></boolean>	0	4/4	Enable/disable low light
				mode.

Group: imagepreview

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
videoin_whitebalance	auto,	auto	4/4	Preview of adjusting white balance of
	manual			image according to mode settings
videoin_restoreatwb	0,1~	0	4/4	Restore of adjusting white balance of
				image according to mode settings
videoin_rgain	0~100	0	4/4	Manual set rgain value of gain control
				setting.
videoin_bgain	0~100	0	4/4	Manual set bgain value of gain control
				setting.

7.13 Exposure window setting per channel

Group: **exposurewin_c<0~(n-1)>** for n channel products **<product dependent>**

(capability	_videoin_	_supportexpwin	= :	1)
-------------	-----------	----------------	-----	----

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
mode	auto, custom, blc	auto	4/4	The mode indicates how to
<product dependent=""></product>				decide the exposure.
				auto: Use full view as the only
				one exposure window.
				custom: Use inclusive and
				exclusive window.
				blc: Use BLC.
win_i<0~9>_enable	<boolean></boolean>	0	4/4	Enable or disable the window.
<product dependent=""></product>				
win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive.
<product dependent=""></product>				1: Indicate inclusive.
win_i<0~9>_home	<coordinate></coordinate>	(150,110)	4/4	Left-top corner coordinate of
<product dependent=""></product>				the window.
win_i<0~9>_size	<window size=""></window>	(100x75)	4/4	Width and height of the
<product dependent=""></product>				window.

Group: exposurewin_c<0~(n-1)>_profile for m profile and n channel product

(capability_videoin_supportexpwin = 1)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
i<0~(m-1)>_mode	auto, custom,	auto	4/4	The mode indicates how to
<product dependent=""></product>	blc			decide the exposure.
				auto: Use full view as the
				only one exposure window.
				custom: Use inclusive and
				exclusive window.
				blc: Use BLC.
i<0~(m-1)>_win_i<0~9>_enable	<boolean></boolean>	0	4/4	Enable or disable the
<product dependent=""></product>				window.
i<0~(m-1)>_win_i<0~9>_policy	0~1	0	4/4	0: Indicate exclusive.
<product dependent=""></product>				1: Indicate inclusive.
i<0~(m-1)>_win_i<0~9>_home	<coordinate></coordinate>	(150,110)	4/4	Left-top corner coordinate of
<product dependent=""></product>				the window.
i<0~(m-1)>_win_i<0~9>_size	<window size=""></window>	(100x75)	4/4	Width and height of the

<product dependent=""></product>		window.

7.14 Audio input per channel

Group: **audioin_c<0~(n-1)>** for n channel products (capability.audioin>0)

				DESCRIPTION
			(get/set)	
source m	micin,	micin	4/4	micin => use built-in microphone
li	inein			input.
				linein => use external
				microphone input.
mute 0), 1	0	4/4	Enable audio mute.
gain 1	L~100	65	4/4	Gain of input.
				(audioin_c<0~(n-1)>_source =
				linein)
boostmic 1	L~100	65	4/4	Enable microphone boost.
				0 => +0dB
				1 => +20dB
				2 => +40dB
				Or
				Gain of input.
				(audioin_c<0~(n-1)>_source =
				micin)
s<0~(m-1)>_codectype a	aac4, g711,	aac4	4/4	Set audio codec type for input.
g	j726			
s<0~(m-1)>_aac4_bitrate 1	L6000,	16000	4/4	Set AAC4 bitrate in bps.
<product dependent=""> 3</product>	32000,			
4	48000,			
6	54000,			
9	96000,			
1	L28000			
s<0~(m-1)>_g711_mode p	ocmu,	pcmu	4/4	Set G.711 mode.
<product dependent=""> p</product>	оста			
s<0~(m-1)>_g726_bitrate 1	L6000,	32000	4/4	Set G.726 bitrate in bps.
<product dependent=""> 2</product>	24000,			
3	32000,			
	10000			
s<0~(m-1)>_g726	ittle, big	little	4/4	Set G.726 bit streaming packing
_bitstreampackingmode	_			mode
<product dependent=""></product>				

s<0~(m-1)>_g726	0, 1	0	4/4	Enable vlcmode for G.726
_vlcmode				
<product dependent=""></product>				

7.15 Time Shift settings

Group: **timeshift**, c for n channel products, m is stream number (capability.timeshift > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	4/4	Enable time shift streaming.
c<0~(n-1)>_s<0~	<boolean></boolean>	0	4/4	Enable time shift streaming for specific
(m-1)>_allow				stream.

7.16 Motion detection settings

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	4/4	Enable motion detection.
win_i<0~4>_enable	<boolean></boolean>	0	4/4	Enable motion window 1~3.
win_i<0~4>_name	string[14]	<blank></blank>	4/4	Name of motion window $1 \sim 3$.
win_i<0~4>_polygon	0 ~ 320,0 ~	0	4/4	Coordinate of polygon window
	240, 0 ~			position.
	320,0 ~			(4 points:
	240, 0 ~			x0,y0,x1,y1,x2,y2,x3,y3)
	320,0 ~			
	240, 0 ~			
	320,0 ~ 240			
win_i<0~4>_objsize	0 ~ 100	0	4/4	Percent of motion detection
				window.
win_i<0~4>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion detection
				window.

Group: motion_c<0~(n-1)> for n channel product

Group: motion_c<0~(n-1)>_profile for m profile and n channel product (capability.nmotionprofile > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
i<0~(m-1)>_enable	<boolean></boolean>	0	4/4	Enable profile 1 \sim
				(m-1).
i<0~(m-1)>_policy	day,	night	4/4	The mode which the

	night,			profile is applied to.
	schedule			
i<0~(m-1)>_begintime	hh:mm	18:00	4/4	Begin time of schedule
				mode.
i<0~(m-1)>_endtime	hh:mm	06:00	4/4	End time of schedule
				mode.
i<0~(m-1)>_win_i<0~4>_enable	<boolean></boolean>	0	4/4	Enable motion
				window.
i<0~(m-1)>_win_i<0~4>_name	string[14]	<blank></blank>	4/4	Name of motion
				window.
i<0~(m-1)>_win_i<0~4>_ polygon	0 ~ 320,0 ~	0	4/4	Coordinate of polygon
	240, 0 ~ 320,0			window position.
	~ 240, 0 ~			(4 points:
	320,0 ~ 240, 0			x0,y0,x1,y1,x2,y2,x3,
	~ 320,0 ~ 240			y3)
i<0~(m-1)>_win_i<0~4>_objsize	0 ~ 100	0	4/4	Percent of motion
				detection window.
i<0~(m-1)>_win_i<0~4>_sensitivity	0 ~ 100	0	4/4	Sensitivity of motion
				detection window.

7.17 Tempering detection settings

Group: **tampering_c<0~(n-1)>** for n channel product (capability.tampering > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	4/4	Enable or disable tamper detection.
threshold	0 ~ 255	32	1/6	Threshold of tamper detection.
duration	10 ~ 600	10	4/4	If tampering value exceeds the 'threshold' for
				more than 'duration' second(s), then tamper
				detection is triggered.

7.18 DDNS

Group: **ddns** (capability.ddns > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable or disable the dynamic DNS.
provider	Safe100,	DyndnsDyn	6/6	Safe100 => safe100.net
	DyndnsDynamic,	amic		DyndnsDynamic => dyndns.org

	1		1	1
	DyndnsCustom,			(dynamic)
	CustomSafe100,			DyndnsCustom => dyndns.org
	<product< td=""><td></td><td></td><td>(custom)</td></product<>			(custom)
	dependent>			CustomSafe100 =>
				Custom server using safe100 method
				<product dependent=""></product>
<provider>_ho</provider>	string[128]	<blank></blank>	6/6	Your DDNS hostname.
stname				
<provider>_us</provider>	string[64]	<blank></blank>	6/6	Your user name or email to login to
ernameemail				the DDNS service provider
<provider>_pa</provider>	string[64]	<blank></blank>	6/6	Your password or key to login to the
sswordkey				DDNS service provider.
<provider>_se</provider>	string[128]	<blank></blank>	6/6	The server name for safe100.
rvername				(This field only exists if the provider is
				customsafe100)

7.19 Express link

Group: expresslink

PARAMETER	VALUE	Default	SECURITY (get/set)	DESCRIPTION
enable	<boolean></boolean>	0	6/6	Enable or disable express link.
state	onlycheck, onlyoffline, checkonline, badnetwork	NULL	-, -	Camera will check the status of network environment and express link URL
url	string[64]	NULL	6/6	The url user define to link to camera

7.20 UPnP presentation

Group: upnppresentation

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	1	6/6	Enable or disable the UPnP
				presentation service.

7.21 UPnP port forwarding

Group: upnpportforwarding

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Enable or disable the UPnP port
				forwarding service.
upnpnatstatus	0~3	0	6/7	The status of UPnP port forwarding,
				used internally.
				0 = OK, 1 = FAIL, 2 = no IGD router,
				3 = no need for port forwarding

7.22 System log

Group: syslog

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enableremotelog	<boolean></boolean>	0	6/6	Enable remote log.
serverip	<ip address=""></ip>	<blank></blank>	6/6	Log server IP address.
serverport	514,	514	6/6	Server port used for log.
	1025~65535			
level	0~7	6	6/6	Levels used to distinguish the
				importance of the
				information:
				0: LOG_EMERG
				1: LOG_ALERT
				2: LOG_CRIT
				3: LOG_ERR
				4: LOG_WARNING
				5: LOG_NOTICE
				6: LOG_INFO
				7: LOG_DEBUG
setparamlevel	0~2	0	6/6	Show log of parameter
				setting.
				0: disable
				1: Show log of parameter
				setting set from external.
				2. Show log of parameter
				setting set from external and

7.23 camera PTZ control

Group: **camctrl** (capability.camctrl.httptunnel > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enablehttptunnel	<boolean></boolean>	0	4/4	Enable HTTP tunnel for
				camera control.

Group: camctrl_c<0~(n-1)> for n channel product (capability.ptzenabled)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
panspeed	-5 ~ 5	0	1/4	Pan speed
tiltspeed	-5 ~ 5	0	1/4	Tilt speed
zoomspeed	-5 ~ 5	0	1/4	Zoom speed
focusspeed	-5 ~ 5	0	1/4	Auto focus speed
patrolseq	string[64]	<blank></blank>	1/4	(For external device)
				The indexes of patrol points,
				separated by ","
patroldwelling	string[128]	<blank></blank>	1/4	(For external device)
				The dwelling time of each patrol
				point, separated by ","
preset_i<0~(npreset-1	string[40]	<blank></blank>	1/4	Name of the preset location.
)>_name				
preset_i<0~(npreset-1	0 ~ 999	0	1/4	The dwelling time of each preset
)>_ dwelling				location
uart	0 ~ (m-1), m	0	1/4	Select corresponding uart
	is UART count			(capability.nuart>0).
cameraid	0~255	0	1/4	Camera ID controlling external
				PTZ camera.
isptz	0 ~ 2	0	1/4	0: disable PTZ commands.
				1: enable PTZ commands with
				PTZ driver.
				2: enable PTZ commands with
				UART tunnel.
disablemdonptz	<boolean></boolean>	0	1/4	Disable motion detection on PTZ
				operation.

7.24 UART control

Group: **uart** (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
ptzdrivers_i<0~19,	string[40]	<product< td=""><td>1/4</td><td>Name of the PTZ driver.</td></product<>	1/4	Name of the PTZ driver.
127>_name		dependent>		
ptzdrivers_i<0~19,	string[128]	< product	1/4	Full path of the PTZ driver.
127>_location		dependent >		
enablehttptunnel	<boolean></boolean>	0	4/4	Enable HTTP tunnel channel to
				control UART.

Group: **uart_i<0~(n-1)>** n is uart port count (capability.nuart > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
baudrate	110,300,600,120	9600	4/4	Set baud rate of COM port.
	0,2400,3600,480			
	0,7200,9600,192			
	00,38400,57600,			
	115200			
databit	5,6,7,8	8	4/4	Data bits in a character frame.
	6,7,8			
	<product< td=""><td></td><td></td><td></td></product<>			
	dependent>			
paritybit	none,	none	4/4	For error checking.
	odd,			
	even			
stopbit	1,2	1	4/4	1
				2-1.5 , data bit is 5
				2-2
uartmode	rs485,	rs485	4/4	RS485 or RS232.
	rs232			
customdrvcmd_i<0~	string[128]	<blank></blank>	1/4	PTZ command for custom
9>				camera.
speedlink_i<0~4>_n	string[40]	<blank></blank>	1/4	Additional PTZ command name.
ame				
speedlink_i<0~4>_c	string[128]	<blank></blank>	1/4	Additional PTZ command list.
md				
ptzdriver	0~19,	128	4/4	The PTZ driver is used by this

127 (custom),	(no driver)	COM	M port.
128 (no driver)			

7.25 SNMP

Group: **snmp** (capability.snmp > 0)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
v2	0~1	0	6/6	SNMP v2 enabled. 0 for disable, 1
				for enable
v3	0~1	0	6/6	SNMP v3 enabled. 0 for disable, 1
				for enable
secnamerw	string[31]	Private	6/6	Read/write security name
secnamero	string[31]	Public	6/6	Read only security name
authpwrw	string[8~128]	<blank></blank>	6/6	Read/write authentication
				password
authpwro	string[8~128]	<blank></blank>	6/6	Read only authentication password
authtyperw	MD5,SHA	MD5	6/6	Read/write authentication type
authtypero	MD5,SHA	MD5	6/6	Read only authentication type
encryptpwrw	string[8~128]	<blank></blank>	6/6	Read/write passwrd
encryptpwro	string[8~128]	<blank></blank>	6/6	Read only password
encrypttyperw	DES	DES	6/6	Read/write encryption type
encrypttypero	DES	DES	6/6	Read only encryption type
rwcommunity	string[31]	Private	6/6	Read/write community
rocommunity	string[31]	Public	6/6	Read only community
syslocation	0~128	<blank></blank>	6/6	System location
syscontact	0~128	<blank></blank>	6/6	System contact

7.26 Layout configuration

Group: layout (New version)

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
logo_default	<boolean></boolean>	1	1/6	0 => Custom logo
				1 => Default logo
logo_link	string[64]	<u>http://ww</u>	1/6	Hyperlink of the logo
		<u>w.vivotek.c</u>		
		<u>om</u>		
logo_powerbyvvtk_hidden	<boolean></boolean>	0	1/6	0 => display the power by
				vivotek logo
				1 => hide the power by vivotek
				logo
custombutton_manualtrigger_s	<boolean></boolean>	1	1/6	Show or hide manual trigger
how				(VI) button in homepage
<product dependent=""></product>				0 -> Hidden
				1 -> Visible
theme_option	1~4	1	1/6	1~3: One of the default
				themes.
				4: Custom definition.
theme_color_font	string[7]	#ffffff	1/6	Font color
theme_color_configfont	string[7]	#ffffff	1/6	Font color of configuration area.
theme_color_titlefont	string[7]	#098bd6	1/6	Font color of video title.
theme_color_controlbackgroun	string[7]	#565656	1/6	Background color of control
d				area.
theme_color_configbackground	string[7]	#323232	1/6	Background color of
				configuration area.
theme_color_videobackground	string[7]	#565656	1/6	Background color of video area.
theme_color_case	string[7]	#323232	1/6	Frame color

7.27 Privacy mask

Group: privacymask_c<0~(n-1)> for n channel product

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	4/4	Enable privacy mask.

174 - User's Manual

win_i<0~4>_enable	<boolean></boolean>	0	4/4	Enable privacy mask
				window.
win_i<0~4>_name	string[14]	<blank></blank>	4/4	Name of the privacy mask
				window.
win_i<0~4>_	0 ~ 320,0 ~ 240,	0	4/4	Coordinate of polygon
polygon	0 ~ 320,0 ~ 240,			window position.
	0 ~ 320,0 ~ 240,			(4 points:
	0 ~ 320,0 ~ 240			x0,y0,x1,y1,x2,y2,x3,y3)

7.28 Capability

Group: capability

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
api_httpversion	<string></string>	0100a	0/7	The HTTP API version.
bootuptime	<positive integer=""></positive>	60	0/7	Server bootup time.
nir	0, <positive integer=""></positive>	0	0/7	Number of IR interfaces. (Recommand to use ir for built-in IR and extir for external IR)
npir	0, <positive integer=""></positive>	0	0/7	Number of PIRs.
ndi	0, <positive integer=""></positive>	1	0/7	Number of digital inputs.
nvi	0, <positive integer=""></positive>	3	0/7	Number of virtual inputs (manual trigger)
ndo	0, <positive integer=""></positive>	1	0/7	Number of digital outputs.
naudioin	0, <positive integer=""></positive>	1	0/7	Number of audio inputs.
naudioout	0, <positive integer=""></positive>	1	0/7	Number of audio outputs.
nvideoin	<positive integer=""></positive>	1	0/7	Number of video inputs.
nmediastream	<positive integer=""></positive>	3	0/7	Number of media stream per channels.
nvideosetting	<positive integer=""></positive>	3	0/7	Number of video settings per channel.
naudiosetting	<positive integer=""></positive>	1	0/7	Number of audio settings per channel.

nuart	0,	0	0/7	Number of UART interfaces.
	<positive integer=""></positive>			
nvideoinprofile	<positive integer=""></positive>	1	0/7	Number of video input
				profiles.
nmotion	0, <positive< td=""><td>5</td><td>0/7</td><td>Number of motion window.</td></positive<>	5	0/7	Number of motion window.
	integer>			
nmotionprofile	0, <positive< td=""><td>1</td><td>0/7</td><td>Number of motion profiles.</td></positive<>	1	0/7	Number of motion profiles.
	integer>			
ptzenabled	0, <positive< td=""><td>189</td><td>0/7</td><td>An 32-bit integer, each bit</td></positive<>	189	0/7	An 32-bit integer, each bit
	integer>			can be set separately as
				follows:
				Bit 0 => Support camera
				control function;
				0(not support), 1(support)
				Bit 1 => Built-in or external
				camera;
				0(external), 1(built-in)
				Bit 2 => Support pan
				operation, 0(not support),
				1(support)
				Bit 3 => Support tilt
				operation; 0(not support),
				1(support)
				Bit 4 => Support zoom
				operation;
				0(not support), 1(support)
				Bit 5 => Support focus
				operation;
				0(not support), 1(support)
				Bit 6 => Support iris
				operation;
				0(not support), 1(support)
				Bit 7 => External or built-in
				PT; 0(built-in), 1(external)
				Bit 8 => Invalidate bit 1 ~
				7;
				0(bit $1 \sim 7$ are valid),
				1(bit 1 \sim 7 are invalid)
				Bit 9 => Reserved bit;
				Invalidate lens_pan,

				Lens_tilt, lens_zoon,
				lens_focus, len_iris.
				0(fields are valid),
				1(fields are invalid)
evctrlchannel	<boolean></boolean>	1	0/7	Indicate whether to support
				HTTP tunnel for
				event/control transfer.
joystick	<boolean></boolean>	0	0/7	Indicate whether to support
Joystick		0	0,7	joystick control.
storage_dbenabled	<boolean></boolean>	1	0/7	Media files are indexed in
storage_ubenableu		1	0/7	database.
		0	0.7	
ptzenabledclient	<boolean></boolean>	0	0/7	Indicate whether to support
				ptz client
protocol_https	< boolean >	1	0/7	Indicate whether to support
				HTTP over SSL.
protocol_rtsp	< boolean >	1	0/7	Indicate whether to support
				RTSP.
protocol_sip	<boolean></boolean>	1	0/7	Indicate whether to support
				SIP.
protocol_maxconnection	<positive integer=""></positive>	10	0/7	The maximum allowed
				simultaneous connections.
protocol_maxgenconnecti	<positive integer=""></positive>	10	0/7	The maximum general
on				streaming connections .
protocol_maxmegaconne	<positive integer=""></positive>	0	0/7	The maximum megapixel
ction				streaming connections.
protocol_rtp_multicast_	<boolean></boolean>	1	0/7	Indicate whether to support
scalable				scalable multicast.
protocol_rtp_multicast_	<boolean></boolean>	0	0/7	Indicate whether to support
backchannel				backchannel multicast.
protocol_rtp_tcp	<boolean></boolean>	1	0/7	Indicate whether to support
				RTP over TCP.
protocol_rtp_http	<boolean></boolean>	1	0/7	Indicate whether to support
				RTP over HTTP.
protocol_spush_mjpeg	<boolean></boolean>	1	0/7	Indicate whether to support
				server push MJPEG.
protocol_snmp	<boolean></boolean>	1	0/7	Indicate whether to support
F				SNMP.
protocol_ipv6	<boolean></boolean>	1	0/7	Indicate whether to support
i		-		IPv6.
		1		11 VO.

videoin_type	0, 1,	2	2	0/7	0 => Interlace	
videom_type	0, 1,	L	2	0, ,	1 => Progress	
					2 => CMOS	
videoin_resolution	<a li<="" td=""><td>st of available</td><td>'192x192,</td><td>0/7</td><td colspan="2">Available resolutions list</td>	st of available	'192x192,	0/7	Available resolutions list	
videoin_resolution	_	ution separated	256x256,	0, ,	Available resol	
		ommas>	384x384,			
	<pre>cl</pre>		512x512,			
		ndent>	768x768,			
	uepe	ndent>	1056x1056,			
			1280x1280,			
			1536x1536			
			1920x1920			
videoin_resolution16x9		st of available	176x144,	0/7	Available 16x9	resolutions
VideoIII_TesolutioII10X9		ution separated	384x216,	0/7	list.	resolutions
		ommas>	640x360,		iist.	
	<pre>content </pre>		1280x720,			
	-	ndent>	1260x720, 1360x768,			
	uepe	ndent>	1600x904,			
			1920x1080			
videoin recelution 1 v1		<a list="" of<="" td=""><td></td><td>0/7</td><td></td><td>Available</td>		0/7		Available
videoin_resolution1x1		available	'192x192,	0/7		
		resolution	256x256,			1x1
			384x384,			resolutions list.
		separated by	512x512,			list.
		commas> <product< td=""><td>768x768,</td><td></td><td></td><td></td></product<>	768x768,			
		-	1056x1056,			
		dependent>	1280x1280,			
			1536x1536			
			1920x1920	0./7		As an iter to be
videoin_nresolution		< number of	9	0/7		Available
		available				resolutions
		resolution				list.
		list>				(only for
		<product< td=""><td></td><td></td><td></td><td>5M series)</td></product<>				5M series)
		dependent>		0/7	A	
videoin_mpeg4_maxframerate		<a list="" of<="" td=""><td>15,15,15,15,</td><td>0/7</td><td>Available maxi</td><td></td>	15,15,15,15,	0/7	Available maxi	
		available	15,15,15,15,		list. (only for 5	or series)
		maximum	15			
		frame rate				
		separated by				
		commas>				

	<product< th=""><th> </th><th></th><th></th></product<>			
	dependent>		0.17	A sette bela service s
videoin_mjpeg_maxframerate	<a list="" of<="" td=""><td>15,15,15,15,</td><td>0/7</td><td>Available maximum frame</td>	15,15,15,15,	0/7	Available maximum frame
	available	15,15,15,15,		list. (only for 5M series)
	maximum	15		
	frame rate			
	separated by			
	commas>			
	<product< td=""><td></td><td></td><td></td></product<>			
	dependent>			
videoin_h264_maxframerate	<a list="" of<="" td=""><td>15,15,15,15,</td><td>0/7</td><td>Available maximum frame</td>	15,15,15,15,	0/7	Available maximum frame
	available	15,15,15,15,		list. (only for 5M series)
	maximum	15		
	frame rate			
	separated by			
	commas>			
	<product< td=""><td></td><td></td><td></td></product<>			
	dependent>			
videoin_streamcodec	< 1 ~ 15,	7,7,7	0/7	Available stream codectype
	1~15, 1~15			(Bit 0 -> mpeg4, Bit 1 ->
	(3 streams) >			mjpeg, Bit 2 -> h264, Bit 3
	<product< td=""><td></td><td></td><td>-> svc). (only for 5M</td></product<>			-> svc). (only for 5M
	dependent>			series)
videoin_fov	<a list="" of<="" td=""><td>1920x1080,1</td><td>0/7</td><td>Available crop size list.</td>	1920x1080,1	0/7	Available crop size list.
	available crop	952x1944		(only for 5M series)
	size separated			
	by commas>			
	<product< td=""><td></td><td></td><td></td></product<>			
	dependent>			
videoin_maxframerate	<a list="" of<="" td=""><td>15,</td><td>0/7</td><td>Available maximum frame</td>	15,	0/7	Available maximum frame
	available	15,		list.
	maximum	15,		
	frame rate	15,		
	separated by	15,		
	commas>	15,		
	<product< td=""><td>15,</td><td></td><td></td></product<>	15,		
	dependent>	15		
videoin_codec	mpeg4.	mpeg4,	0/7	Available codec list.
	mjpeg, h264	mjpeg,		
	<pre>cproduct</pre>	h264		
	· ·		1	1

	dependent>			
videoin_flexiblebitrate	<boolean></boolean>	<product< td=""><td>0/7</td><td>Indicate whether to</td></product<>	0/7	Indicate whether to
	<product< td=""><td>dependent</td><td></td><td>support flexible</td></product<>	dependent		support flexible
	dependent	>		bitrate.
	>			
videoout_codec	<a list="" of="" td="" the<=""><td><blank></blank></td><td>0/7</td><td>Available codec list.</td>	<blank></blank>	0/7	Available codec list.
	available			
	codec types			
	separated by			
	commas)			
	<product< td=""><td></td><td></td><td></td></product<>			
	dependent>			
audio_aec	<boolean></boolean>	0	0/7	Indicate whether to support
				acoustic echo cancellation.
audio_extmic	<boolean></boolean>	1	0/7	Indicate whether to support
				external microphone input.
audio_linein	<boolean></boolean>	1	0/7	Indicate whether to support
				external line input.
				(It will be replaced by
				audio_mic and
				audio_extmic.)
audio_lineout	<boolean></boolean>	1	0/7	Indicate whether to support
				line output.
audio_headphoneout	<boolean></boolean>	0	0/7	Indicate whether to support
				headphone output.
audioin_codec	aac4, g711,	aac4, g711,	0/7	Available codec list for
	g726	g726		audio input.
	<product< td=""><td></td><td></td><td></td></product<>			
	dependent>			
audioout_codec	g711		0/7	Available codec list for SIP.
	<product< td=""><td></td><td></td><td></td></product<>			
	dependent>			
camctrl_httptunnel	<boolean></boolean>	0	0/7	Indicate whether to support
				httptunnel.
camctrl_httptunnelclient	<boolean></boolean>	0	0/7	Indicate whether to support
				httptunnel client.
camctrl_privilege	<boolean></boolean>	1	0/7	Indicate whether to support
				"Manage Privilege" of PTZ
				control in the Security

				page.
				1: support both
				/cgi-bin/camctrl/camctrl.cg
				i and
				/cgi-bin/viewer/camctrl.cgi
				0: support only
				/cgi-bin/viewer/camctrl.cgi
uart_httptunnel	<boolean></boolean>	0	0/7	Indicate whether to support
uart_intiplumer		0	0/7	HTTP tunnel for UART
				transfer.
transmission mode		Tx	0/7	Indicate transmission mode
transmission_mode	Tx,	IX	0/ /	
	Rx,			of the machine: TX =
	Both			server, $Rx =$ receiver box,
			0.7	Both = DVR.
network_wire	<boolean></boolean>	1	0/7	Indicate whether to support
				Ethernet.
network_wireless	<boolean></boolean>	0	0/7	Indicate whether to support
				wireless.
wireless_s802dot11b	<boolean></boolean>	0	0/7	Indicate whether to support
				wireless 802.11b+.
wireless_s802dot11g	<boolean></boolean>	0	0/7	Indicate whether to support
				wireless 802.11g.
wireless_encrypt_wep	<boolean></boolean>	0	0/7	Indicate whether to support
				wireless WEP.
wireless_encrypt_wpa	<boolean></boolean>	0	0/7	Indicate whether to support
				wireless WPA.
wireless_encrypt_wpa2	<boolean></boolean>	0	0/7	Indicate whether to support
				wireless WPA2.
wireless_beginchannel	$1 \sim 14$	255	0/7	Indicate the begin channel
				of wireless network
wireless_endchannel	1 ~ 14	255	0/7	Indicate the end channel of
				wireless network
derivative_brand	<boolean></boolean>	1	0/7	Indicate whether to support
_				the upgrade function for
				the derivative brand. For
				example, if the value is
				true, the VVTK product can
				be upgraded to VVXX.
				(TCVV<->TCXX is
				excepted)
				excepted)

npreset	0, <positive< th=""><th>20</th><th>0/7</th><th>Number of preset locations</th></positive<>	20	0/7	Number of preset locations
	integer>			
eptz	0, <positive< td=""><td>7</td><td>0/7</td><td>A 32-bit integer, each bit</td></positive<>	7	0/7	A 32-bit integer, each bit
	integer>			can be set separately as
				follows:
				Bit 0 => stream 1 supports
				ePTZ or not.
				Bit 1 => stream 2 supports
				ePTZ or not.
				The rest may be deduced
				by analogy
nanystream	0, <positive< td=""><td>0</td><td>0/7</td><td>number of any media</td></positive<>	0	0/7	number of any media
	integer>			stream per channel
iva	<boolean></boolean>	0	0/7	Indicate whether to support
				Intelligent Video analysis
tampering	<boolean></boolean>	1	0/7	Indicate whether to support
		-	0,1	tampering detection.
test_ac	<boolean></boolean>	1	0/7	Indicate whether to support
		-	0,7	test ac key.
version_onvifdaemon	<string></string>	1.7.1.4	0/7	Indicate ONVIF daemon
version_onvitudemon	<sumg></sumg>	1.7.1.4	0/ /	version
image_wdrc	<boolean></boolean>	1	0/7	
iiiage_wuic	< BOOlean>	L	0/7	Indicate whether to support WDR enhanced.
income inich and			0/7	
image_ iristype	<string></string>		0/7	Indicate iris type.
image_ focusassist	<boolean></boolean>	0	0/7	Indicate whether to support
				focus assist.
fisheye	<boolean></boolean>	1	0/7	Indicate fisheye model.
localstorage_manageable	<boolean></boolean>	1	0/7	Indicate whether
				manageable local storage is
				supported.
localstorage_seamless	<boolean></boolean>	1	0/7	Indicate whether seamless
				recording is supported.
localstorage_modnum	0,	4	0/7	The maximum MOD
	<positive< td=""><td></td><td></td><td>connection numbers.</td></positive<>			connection numbers.
	integer>			
adaptiverecording	<boolean></boolean>	1	0/7	Indicate whether to support
			-,	adaptive recording.
adaptivestreaming	<boolean></boolean>	1	0/7	Indicate whether to support
	< DOULCUITZ	1 -	5,7	indicate whether to support

supportsd	<boolean></boolean>	1	0/7	Indicate whether to support
				local storage.
vadp	<positive< td=""><td>19</td><td>0/7</td><td>An 32-bit integer, each bit</td></positive<>	19	0/7	An 32-bit integer, each bit
	integer>			can be set separately as
				follows:
				Bit 0 => VADP Interface
				Bit 1 => Capture video raw
				data
				Bit 2 => Support encode
				jpeg
				Bit 3 => Audio
				Bit 4 => Event
fisheyelocaldewarp_c <n></n>	<integer></integer>	0	0/7	Indicate the supported
				streams of local
				dewarp. One bit
				represents one
				supported stream.
				The LSB indicates
				stream 0.
				Ex: "3" means stream
				0 and stream 1
				support local dewarp.

Group: **capability_videoin_c<n>_localdewarp**, n denotes the channel index, range is from 0 to "capability_nvideoin"-1

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
typeceilingmount	10, 1P, 2P, 1R, 4R	0/7	Available dewarp types of
typeceningmount	<pre><pre>conduct dependent></pre></pre>	0, 7	ceiling and floor mount.
typewallmount	10, 1P, 1R, 4R	0/7	Available dewarp types of wall
	<product dependent=""></product>		mount.
resolutionC1P	640x160, 1280x320,	0/7	Available resolutions of 1P
	1536x384, 1920x480		mode of ceiling and floor
	<product dependent=""></product>		mount.
resolutionC2P	320x320, 640x640,	0/7	Available resolutions of 2P
	1280x1280		mode of ceiling and floor
	<product dependent=""></product>		mount.
resolutionC1R	192x192, 256x256,	0/7	Available resolutions of 1R
	384x384, 512x512,		mode of ceiling and floor
	640x640		mount.

	<product dependent=""></product>		
resolutionC4R	384x384, 512x512,	0/7	Available resolutions of 4R
	768x768, 1088x1088,		mode of ceiling and floor
	1280x1280		mount.
	<product dependent=""></product>		
resolutionW1P	640x320, 1280x640,	0/7	Available resolutions of 1P
	1536x768, 1920x960		mode of wall mount.
	<product dependent=""></product>		
resolutionW1R	192x192, 256x256,	0/7	Available resolutions of 1R
	384x384, 512x512,		mode of wall mount.
	640x640		
	<product dependent=""></product>		
resolutionW4R	384x384, 512x512,	0/7	Available resolutions of 4R
	768x768, 1088x1088,		mode of wall mount.
	1280x1280		
	<product dependent=""></product>		

7.29 Customized event script

Group: event_customtaskfile_i<0~2>

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
name	string[41]	<blank></blank>	6/7	Custom script identification of this
				entry.
date	string[17]	<blank></blank>	6/7	Date of custom script.
time	string[17]	<blank></blank>	6/7	Time of custom script.

7.30 Event setting

Group: event_i<0~2>

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
name	string[40]	<blank></blank>	6/6	Identification of this entry.
enable	0, 1	0	6/6	Enable or disable this event.

priority	0, 1, 2	1	6/6	Indicate the priority of this event:
				"0" = low priority
				"1" = normal priority
				"2" = high priority
delay	1~999	20	6/6	Delay in seconds before detecting the
				next event.
trigger	boot,	boot	6/6	Indicate the trigger condition:
	di,			"boot" = System boot
	motion,			"di"= Digital input
	seq,			"motion" = Video motion detection
	recnotify,			"seq" = Periodic condition
	tampering,			"visignal" = Video input signal loss.
	visignal,			"recnotify" = Recording notification.
	vi			"tampering" = Tamper detection.
				"vi"= Virtual input (Manual trigger)
				"volalarm" = Audio detection.
triggerstatus	String[40]	trigger	6/6	The status for event trigger
di	<integer></integer>	1	6/6	Indicate the source id of di trigger.
				This field is required when trigger
				condition is "di".
				One bit represents one digital input.
				The LSB indicates DI 0.
mdwin	<integer></integer>	0	6/6	Indicate the source window id of
				motion detection.
				This field is required when trigger
				condition is "md".
				One bit represents one window.
				The LSB indicates the 1^{st} window.
				For example, to detect the 1^{st} and 3^{rd}
				windows, set mdwin as 5.
mdwin0	<integer></integer>	0	6/6	Similar to mdwin. The parameter
				takes effect when profile 1 of motion
				detection is enabled.
vi	<integer></integer>	0	6/6	Indicate the source id of vi trigger.
				This field is required when trigger
				condition is "vi".
				One bit represents one digital input.
				The LSB indicates VI 0.

inter	1~999	1	6/6	Interval of snapshots in minutes.
				This field is used when trigger
				condition is "seq".
weekday	0~127	127	6/6	Indicate which weekday is scheduled.
				One bit represents one weekday.
				bit0 (LSB) = Saturday
				bit1 = Friday
				bit2 = Thursday
				bit3 = Wednesday
				bit4 = Tuesday
				bit5 = Monday
				bit6 = Sunday
				For example, to detect events on
				Friday and Sunday, set weekday as
				66.
begintime	hh:mm	00:00	6/6	Begin time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule.
				(00:00 ~ 24:00 sets schedule as
				always on)
lowlightcondition	0,1	1	6/6	Switch on white light LED in low light
<product dependent=""></product>				condition
				0 => Do action at all times
				1 => Do action in low-light conditions
action_do_i<0~(ndo-1)	0,1	0	6/6	Enable or disable trigger digital
>_enable				output.
action_do_i<0~(ndo-1)	1~999	1	6/6	Duration of the digital output trigger
>_duration				in seconds.
action_goto_enable	<boolean></boolean>	0	6/6	Enable/disable ptz goto preset
<product dependent=""></product>				position on event triggered.
action_goto_name	string[40]	<blank></blank>	6/6	Specify the preset name that ptz goto
<product dependent=""></product>				on event triggered.
action_cf_enable	<boolean></boolean>	0	6/6	Enable or disable sending media to
				SD card.
action_cf_folder	string[128]	<blank></blank>	6/6	Path to store media.
action_cf_media	NULL, 0~4	<blank></blank>	6/6	Index of the attached media.
action_cf_datefolder	<boolean></boolean>	0	6/6	Enable this to create folders by date,
				time, and hour automatically.

action_cf_backup	<boolean></boolean>	0	6/6	Enable or disable the function that
				send media to SD card for backup if
				network is disconnected.
action_server_i<0~4>_e	0, 1	0	6/6	Enable or disable this server action.
nable				
action_server_i<0~4>_	NULL, 0~4	<blank></blank>	6/6	Index of the attached media.
media				
action_server_i<0~4>_	<boolean></boolean>	0	6/6	Enable this to create folders by date,
datefolder				time, and hour automatically.
action_patrol_enable	<boolean></boolean>	0	6/6	Enable/disable ptz patrol when event
(only for VS series)				triggered.
<product dependent=""></product>				
action_ patrol _server	0~255	0	6/6	Indicate the target servers to which
(only for VS series)				the snapshots taken during patrol
<product dependent=""></product>				dwelling time should be sent.
				One bit represents one application
				server (server_i0~i4).
				bit0 (LSB) = server_i0.
				bit1 = server_i1.
				bit2 = server_i2.
				bit3 = server_i3.
				bit4 = server_i4.
				For example, enable server_i0,
				server_i2, and server_i4 as
				notification servers; the notifyserver
				value is 21.

7.31 Server setting for event action

Group: **server_i**<0~4>

PARAMETER	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
name	string[40]	NULL	6/6	Identification of this entry
type	email,	email	6/6	Indicate the server type:
	ftp,			"email" = email server
	http,			"ftp" = FTP server
	ns			"http" = HTTP server
				"ns" = network storage
http_url	string[128]	http://	6/6	URL of the HTTP server to upload.

http_username	string[64]	NULL	6/6	Username to log in to the server.
http_passwd	string[64]	NULL	6/6	Password of the user.
ftp_address	string[128]	NULL	6/6	FTP server address.
ftp_username	string[64]	NULL	6/6	Username to log in to the server.
ftp_passwd	string[64]	NULL	6/6	Password of the user.
ftp_port	0~65535	21	6/6	Port to connect to the server.
ftp_location	string[128]	NULL	6/6	Location to upload or store the media.
ftp_passive	0, 1	1	6/6	Enable or disable passive mode.
				0 = disable passive mode
				1 = enable passive mode
email_address	string[128]	NULL	6/6	Email server address.
email_sslmode	0, 1	0	6/6	Enable support SSL.
email_port	0~65535	25	6/6	Port to connect to the server.
email_username	string[64]	NULL	6/6	Username to log in to the server.
email_passwd	string[64]	NULL	6/6	Password of the user.
email_senderemail	string[128]	NULL	6/6	Email address of the sender.
email_recipientemail	string[128]	NULL	6/6	Email address of the recipient.
ns_location	string[128]	NULL	6/6	Location to upload or store the media.
ns_username	string[64]	NULL	6/6	Username to log in to the server.
ns_passwd	string[64]	NULL	6/6	Password of the user.
ns_workgroup	string[64]	NULL	6/6	Workgroup for network storage.

7.32 Media setting for event action

Group: **media_i<0~4>** (media_freespace is used internally.)

PARAMETER	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
name	string[40]	NULL	6/6	Identification of this entry
	snapshot, systemlog, videoclip, recordmsg	snapshot	-	Media type to send to the server or store on the server.

snapshot_source	<integer></integer>	0	6/6	Indicate the source of media stream.
	5		,	0 means the first stream.
				1 means the second stream and etc.
				2 means the third stream and etc.
				3 means the fourth stream and etc.
snapshot_prefix	string[16]	Snapshot1_	6/6	Indicate the prefix of the filename.
				media_i0=> Snapshot1_
				media_i1=> Snapshot2_
				media_i2=> Snapshot3_
				media_i3=> Snapshot4_
				media_i4=> Snapshot5_
snapshot_datesuffix	0, 1	0	6/6	Add date and time suffix to filename:
				1 = Add date and time suffix.
				0 = Do not add.
snapshot_preevent	0 ~ 7	1	6/6	Indicates the number of pre-event
				images.
snapshot_postevent	0 ~ 7	1	6/6	The number of post-event images.
videoclip_source	<integer></integer>	0	6/6	Indicate the source of media stream.
				0 means the first stream.
				1 means the second stream and etc.
				2 means the third stream and etc.
				3 means the fourth stream and etc.
videoclip_prefix	string[16]	VideoClip1_	6/6	Indicate the prefix of the filename.
videoclip_preevent	0~9	0	6/6	Indicates the time for pre-event
				recording in seconds.
videoclip_maxduration	1 ~ 20	5	6/6	Maximum duration of one video clip in
				seconds.
videoclip_maxsize	50 ~ 8192	1000	6/6	Maximum size of one video clip file in
				Kbytes.

7.33 Recording

Group: recording_i<0~1>

PARAMETER	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
name	string[40]	NULL	6/6	Identification of this entry.
trigger	schedule, networkfail	schedule	6/6	The event trigger type schedule: The event is triggered by schedule networkfail: The event is triggered by the failure of network connection.
enable	0, 1	0	6/6	Enable or disable this recording.
priority	0, 1, 2	1	6/6	Indicate the priority of this recording: "0" indicates low priority. "1" indicates normal priority. "2" indicates high priority.
source	0~3	0	6/6	Indicate the source of media stream. 0 means the first stream. 1 means the second stream and so on.
limitsize	0,1	0	6/6	0: Entire free space mechanism 1: Limit recording size mechanism
cyclic	0,1	0	6/6	0: Disable cyclic recording 1: Enable cyclic recording
notify	0,1	1	6/6	0: Disable recording notification 1: Enable recording notification

potificor or	0~31	0	C IC	Indicate which patification convertion
notifyserver	0~31	0	6/6	Indicate which notification server is scheduled.
				One bit represents one application
				server (server_i0~i4).
				bit0 (LSB) = server_i0.
				bit1 = server_i1.
				bit2 = server_i2.
				bit3 = server_i3.
				bit4 = server_i4.
				For example, enable server_i0,
				server_i2, and server_i4 as
				notification servers; the notifyserver
				value is 21.
weekday	0~127	127	6/6	Indicate which weekday is scheduled.
				One bit represents one weekday.
				bit0 (LSB) = Saturday
				bit1 = Friday
				bit2 = Thursday
				bit3 = Wednesday
				bit4 = Tuesday
				bit5 = Monday
				bit6 = Sunday
				For example, to detect events on
				Friday and Sunday, set weekday as
				66.
begintime	hh:mm	00:00	6/6	Start time of the weekly schedule.
endtime	hh:mm	24:00	6/6	End time of the weekly schedule.
				(00:00~24:00 indicates schedule
				always on)
prefix	string[16]	<blank></blank>	6/6	Indicate the prefix of the filename.
cyclesize	200~	100	6/6	The maximum size for cycle recording
				in Kbytes when choosing to limit
				recording size.
				(not used in FE8171)
reserveamount	0~	100	6/6	The reserved amount in Mbytes when
				choosing cyclic recording mechanism.
L				

dest	cf,	cf	6/6	The destination to store the recorded
	0~4			data.
				"cf" means local storage (CF or SD
				card).
				"0" means the index of the network
				storage.
cffolder	string[128]	NULL	6/6	Folder name.
filesize	100~900	100	6/6	Unit: Mega bytes.
				When this condition is reached,
				recording file is truncated.
duration	1~30	1	6/6	Uuit: Minute
				When this condition is reached,
				recording file is truncated.
adaptive_enable	0,1	0	6/6	Indicate whether the adaptive
<product dependent=""></product>				recording is enabled
adaptive_preevent	0~9	1	6/6	Indicate when is the adaptive
<product dependent=""></product>				recording started before the event
				trigger point (seconds)
adaptive_postevent	0~10	1	6/6	Indicate when is the adaptive
<product dependent=""></product>				recording stopped after the event
				trigger point (seconds)

7.34 HTTPS

Group: **https** (capability.protocol.https > 0)

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
enable	<boolean></boolean>	0	6/6	To enable or disable secure
				HTTP.
policy	<boolean></boolean>	0	6/6	If the value is 1, it will force
				HTTP connection redirect to
				HTTPS connection
method	auto,	auto	6/6	auto => Create self-signed
	manual,			certificate automatically.
	install			manual => Create self-signed
				certificate manually.
				install => Create certificate
				request and install.
status	-3 ~ 1	0	6/7	Specify the https status.

				-3 = Certificate not installed
				-2 = Invalid public key
				-1 = Waiting for certificate
				0 = Not installed
				1 = Active
countryname	string[2]	тw	6/6	Country name in the certificate
				information.
stateorprovincename	string[128]	Asia	6/6	State or province name in the
				certificate information.
localityname	string[128]	Asia	6/6	The locality name in the
				certificate information.
organizationname	string[64]	Vivotek.Inc	6/6	Organization name in the
				certificate information.
unit	string[32]	Vivotek.Inc	6/6	Organizational unit name in the
				certificate information.
commonname	string[64]	www.vivotek.	6/6	Common name in the certificate
		com		information.
validdays	0 ~ 3650	3650	6/6	Valid period for the certification.

7.35 Storage management setting

Currently it's for local storage (SD, CF card)

Group: **disk_i<0~(n-1)>** n is the total number of storage devices. (capability.storage.dbenabled > 0)

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
cyclic_enabled	<boolean></boolean>	0	6/6	Enable cyclic storage method.
autocleanup_enabled	<boolean></boolean>	0	6/6	Enable automatic clean up method. Expired and not locked media files will be deleted.
autocleanup_maxage	<positive< td=""><td>7</td><td>6/6</td><td>To specify the expired days for</td></positive<>	7	6/6	To specify the expired days for
	integer>			automatic clean up.

7.36 ePTZ setting

Group: **eptz_c<0~(n-1)>** for n channel product. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
tiltspeed	-5 ~ 5	0	1/4	Tilt speed
panspeed	-5 ~ 5	0	1/4	Pan speed

zoomspeed	-5 ~ 5	0	1/4	Zoom speed
panoramicspeed	1 ~ 5	1	1/4	Panoramic speed
rotatespeed	1 ~ 5	1	1/4	Rotate speed

Group: **eptz_c<0~(n-1)>_s<0~(m-1)>** for n channel product and m is the number of streams which support ePTZ. (capability.eptz > 0)

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
patrolseq	string[120]	<blank></blank>	1/4	The patrol sequence of ePTZ. All the
				patrol position indexes will be
				separated by ","
preset_i<0~19>_name	string[40]	<blank></blank>	1/4	Name of ePTZ preset.
preset_i<0~19>_pos	<coordinate></coordinate>	<blank></blank>	1/4	Coordinate of the preset.
				(It should be get from plugin: x, y, z,
				zfactor, scroll)

7.37 Fisheye info

Group: fisheyeinfo

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
revisedcenteraxis	<coordinate></coordinate>	<product< td=""><td>6/99</td><td>The actual center axis</td></product<>	6/99	The actual center axis
		dependent>		coordinate
radius	<integer></integer>	<product< td=""><td>6/99</td><td>The actual center radius</td></product<>	6/99	The actual center radius
		dependent>		

7.38 Seamless recording setting

Group: **seamlessrecording** (capability.localstorage.seamless > 0)

PARAMETER	VALUE	Default	SECURITY	DESCRIPTION
			(get/set)	
diskmode	seamless,	seamless	1/6	"seamless" indicates enable seamless
	manageable			recording.
				"manageable" indicates disable
				seamless recording.
maxconnection	3	3	1/6	Maximum number of connected
				seamless streaming.
stream	1~3	3	1/6	(Internal used, read only)

output	0~3	2	1/6	(Internal used, read only)
enable	<boolean></boolean>	0	1/6	Indicate whether seamless recording is recording to local storage or not at present. (Read only)
guid<0~2>_id	string[127]	<blank></blank>	1/6	The connected seamless streaming ID. (Read only)
guid<0~2>_number	0~3	0	1/6	Number of connected seamless streaming with guid<0~2>_id. (Read only)

7.39 genetec info

Group: genetec

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
image_contrast	<integer></integer>	<product< td=""><td>6/6</td><td>Only for genetec omnicast</td></product<>	6/6	Only for genetec omnicast
		dependent>		
image_brightness	<integer></integer>	<product< td=""><td>6/6</td><td>Only for genetec omnicast</td></product<>	6/6	Only for genetec omnicast
		dependent>		
motion_i<0~4>	<integer></integer>	<product< td=""><td>6/6</td><td>Only for genetec omnicast</td></product<>	6/6	Only for genetec omnicast
		dependent>		

7.40 VIVOTEK Application Development Platform setting

Group: vadp

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
version	<string></string>	<product< td=""><td>6/7</td><td>Indicate the VADP version.</td></product<>	6/7	Indicate the VADP version.
		dependent>		
resource_total_video	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate total video resource</td></product<>	6/7	Indicate total video resource
		dependent>		number of the system.
resource_total_audio	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate total audio resource</td></product<>	6/7	Indicate total audio resource
		dependent>		number of the system.
resource_total_do	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate total DO resource</td></product<>	6/7	Indicate total DO resource
		dependent>		number of the system.
resource_total_memory	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate total available</td></product<>	6/7	Indicate total available
		dependent>		memory size for VADP

				modules.
resource_total_storage	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate total size of the</td></product<>	6/7	Indicate total size of the
		dependent>		internal storage space for
				storing VADP modules.
resource_free_video	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate free video resource</td></product<>	6/7	Indicate free video resource
		dependent>		number of the system.
resource_free_audio	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate free audio resource</td></product<>	6/7	Indicate free audio resource
		dependent>		number of the system.
resource_free_do	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate free DO resource</td></product<>	6/7	Indicate free DO resource
		dependent>		number of the system.
resource_free_memory	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate free memory size</td></product<>	6/7	Indicate free memory size
		dependent>		for VADP modules.
resource_free_storage	<integer></integer>	<product< td=""><td>6/7</td><td>Indicate current free storage</td></product<>	6/7	Indicate current free storage
		dependent>		size for uploading VADP
				modules.
module_number	<integer></integer>	0	6/7	Record the total module
				number that already stored
				in the system.
module_order	string[40]	<blank></blank>	6/6	The execution order of the
				enabled modules.
module_save2sd	<boolean></boolean>	<product< td=""><td>6/6</td><td>Indicate if the module</td></product<>	6/6	Indicate if the module
		dependent>		should be saved to SD card
				when user want to upload it.
				If the value is false, save
				module to the internal
				storage space and it will
				occupy storage size.

Group: vadp_module_i<0~(n-1)>

NAME	VALUE	DEFAULT	SECURITY	DESCRIPTION
			(get/set)	
enable	<boolean></boolean>	0	6/6	Indicate if the module is
				enabled or not.
				If yes, also add the index of
				this module to the
				module_order.
name	string[40]	<blank></blank>	6/6	Module name
url	string[120]	<blank></blank>	6/6	Define the URL string after
				the IP address if the module
				provides it own web page.

vender	string[40]	<blank></blank>	6/6	The provider of the module.
vendorurl	string[120]	<blank></blank>	6/6	URL of the vendor.
version	string[40]	<blank></blank>	6/6	Version of the module.
license	string[40]	<blank></blank>	6/6	Indicate the license status of
				the module.
path	string[40]	<blank></blank>	6/6	Record the storage path of
				the module.
initscr	string[40]	<blank></blank>	6/6	The script that will handle
				operation commands from
				the system.
status	string[40]	<blank></blank>	6/6	Indicate the running status
				of the module.

7.41 Fisheye local dewarp setting

Group: **fisheyedewarp_c<n>**, where $n = channel index from 0 \sim "capability_nvideoin"-1$

NAME	VALUE	DEFAULT	SECURITY (get/set)	DESCRIPTION
panspeed	-5 ~ 5	0	1/4	Pan speed of regional view
panspeed		0	1/ 4	Tan speed of regional view
	<integer< td=""><td></td><td></td><td></td></integer<>			
	>			
tiltspeed	-5 ~ 5	0	1/4	Tilt speed of regional view
	<integer< td=""><td></td><td></td><td></td></integer<>			
	>			
zoomspeed	-5 ~ 5	0	1/4	Zoom speed of regional
	<integer< td=""><td></td><td></td><td></td></integer<>			
	>			
s<0~(m-1)>_panoram	0~359	0	1/4	Initial pan position of panorama view.
a_panstart	<integer< td=""><td></td><td></td><td>(only available for 1P and 2P mode at</td></integer<>			(only available for 1P and 2P mode at
	>			ceiling or floor mount)
s<0~(m-1)>_region_p	-90~359	315	1/4	Pan home angle of regional view
an	<integer< td=""><td></td><td></td><td>Pan range of ceiling/floor mount is</td></integer<>			Pan range of ceiling/floor mount is
	>			[0~359].
				Pan range of wall mount is [-90~90].
s<0~(m-1)>_region_til	-90~90	45	1/4	Tilt home angle of regional view
t	<integer< td=""><td></td><td></td><td>Tilt range of ceiling/floor mount is</td></integer<>			Tilt range of ceiling/floor mount is
	>			[0~90].
				Tilt range of wall mount is
				[-90~90].
s<0~(m-1)>_region_zo	100~300	100	1/4	Zoom home ratio of regional view

om	<integer< th=""><th></th><th>]</th></integer<>]
	>		

8. Useful Functions

8.1 Drive the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges. **Method:** GET/POST

Syntax:	
http://< <i>servername</i> >/cgi-bin/dido/setdo.cgi?do1=< <i>state</i> >[&do2= <state>]</state>	
[&do3= <state>][&do4=<state>]</state></state>	

Where state is 0 or 1; "0" means inactive or normal state, while "1" means active or triggered state.

PARAMETER	VALUE	DESCRIPTION
do <num></num>	0, 1	0 – Inactive, normal state
		1 – Active, triggered state

Example: Drive the digital output 1 to triggered state and redirect to an empty page.

http://myserver/cgi-bin/dido/setdo.cgi?do1=1

8.2 Query Status of the Digital Input (capability.ndi > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://<servername>/cgi-bin/dido/getdi.cgi?[di0][&di1][&di2][&di3]

If no parameter is specified, all of the digital input statuses will be returned.

Return:

HTTP/1.0 200 OK\r\n
Content-Type: text/plain\r\n
Content-Length: < <i>length</i> >\r\n
\r\n
[di0= <state>]\r\n</state>
[di1= <state>]\r\n</state>
[di2= <state>]\r\n</state>
[di3= <state>]\r\n</state>

where <*state*> can be 0 or 1.

Example: Query the status of digital input 1 .

Request: http://myserver/cgi-bin/dido/getdi.cgi?di1 Response: HTTP/1.0 200 OK\r\n Content-Type: text/plain\r\n Content-Length: 7\r\n \r\n di1=1\r\n

8.3 Query Status of the Digital Output (capability.ndo > 0)

Note: This request requires Viewer privileges

Method: GET/POST

Syntax:

http://<servername>/cgi-bin/dido/getdo.cgi?[do0][&do1][&do2][&do3]

If no parameter is specified, all the digital output statuses will be returned.

Return: HTTP/1.0 200 OK\r\n Content-Type: text/plain\r\n Content-Length: <*length*>\r\n \r\n [do0=<state>]\r\n [do1=<state>]\r\n [do2=<state>]\r\n [do3=<state>]\r\n

where <*state*> can be 0 or 1.

Example: Query the status of digital output 1.

Request: http://myserver/cgi-bin/dido/getdo.cgi?do1 Response: HTTP/1.0 200 OK\r\n Content-Type: text/plain\r\n

.

Content-Length: 7\r\n

\r\n do1=1\r\n

8.4 3D Privacy Mask

Note: This request requires admin user privilege

<SD81X1> You can set privacy mask only at zoom 1x. To go back to zoom 1x directly, please send this cgi command: "/cgi-bin/camctrl/camposition.cgi?setzoom=0" Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/admin/setpm3d.cgi?method=<value>&name=<value>&[maskheight=<value>& maskwidth=<value>&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
method	add	Add a 3D privacy mask at current location
	delete	Delete a 3D privacy mask
	edit	Edit a 3D privacy mask
maskname	string[40]	3D privacy mask name
maskheight	integer	3D privacy mask height
maskwidth	integer	3D privacy mask width
return	<return page=""></return>	Redirect to page < <i>return page</i> > after the 3D privacy mask is
		configured. The < <i>return page</i> > can be a full URL path or
		relative path according to the current path. If you omit this
		parameter, it will redirect to an empty page.

8.5 Capture Single Snapshot

Note: This request requires Normal User privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/viewer/video.jpg?[channel=<value>][&resolution=<value>]
[&quality=<value>][&streamid=<value>]
```

If the user requests a size larger than all stream settings on the server, this request will fail.

PARAMETER	VALUE	DEFAULT	DESCRIPTION
channel	0~(n-1)	0	The channel number of the video source.
resolution	<available< td=""><td>0</td><td>The resolution of the image.</td></available<>	0	The resolution of the image.

	resolution>		
quality	1~5	3	The quality of the image.
streamid	0~(m-1)	<product< td=""><td>The stream number.</td></product<>	The stream number.
		dependent>	

The server will return the most up-to-date snapshot of the selected channel and stream in JPEG format. The size and quality of the image will be set according to the video settings on the server.

HTTP/1.0 200 OK\r\n	
Construct Theorem internet (in a shall a	
Content-Type: image/jpeg\r\n	
[Content-Length: <image size=""/> \r\n]	

8.6 Account Management

Note: This request requires Administrator privileges.

Method: GET/POST

Syntax:

http://<servername>/cgi-bin/admin/editaccount.cgi?

method=<value>&username=<name>[&userpass=<value>][&privilege=<value>]

[&privilege=<value>][...][&return=<return page>]

PARAMETER	VALUE	DESCRIPTION
method	Add	Add an account to the server. When using this method, the
		"username" field is necessary. It will use the default value of
		other fields if not specified.
	Delete	Remove an account from the server. When using this method,
		the "username" field is necessary, and others are ignored.
	edit	Modify the account password and privilege. When using this
		method, the "username" field is necessary, and other fields are
		optional. If not specified, it will keep the original settings.
username	<name></name>	The name of the user to add, delete, or edit.
userpass	<value></value>	The password of the new user to add or that of the old user to
		modify. The default value is an empty string.
Privilege	<value></value>	The privilege of the user to add or to modify.
	viewer	Viewer privilege.

	operator	Operator privilege.
	admin	Administrator privilege.
Return	<return page=""></return>	Redirect to the page < return page > after the parameter is
		assigned. The < <i>return page</i> > can be a full URL path or relative
		path according to the current path. If you omit this parameter, it
		will redirect to an empty page.

8.7 System Logs

Note: This request require Administrator privileges. **Method:** GET/POST

Syntax:

http://<servername>/cgi-bin/admin/syslog.cgi

Server will return the most up-to-date system log.

Return:

HTTP/1.0 200 OK\r\n Content-Type: text/plain\r\n Content-Length: <syslog length>\r\n \r\n <system log information>\r\n

8.8 Upgrade Firmware

Note: This request requires Administrator privileges.

Method: POST

Syntax:

http://<servername>/cgi-bin/admin/upgrade.cgi

Post data:

fimage=<file name>[&return=<return page>]\r\n \r\n <multipart encoded form data>

Server will accept the file named <file name> to upgrade the firmware and return with <return page> if indicated.

8.9 Camera Control (capability.ptzenabled, not used in FE8174)

Note: This request requires Viewer privileges. **Method:** GET/POST

Syntax:

http://< <i>servername</i> >/cgi-bin/viewer/camctrl.cgi?[channel= <value>][&camid=<value>]</value></value>
[&move= <value>] - Move home, up, down, left, right</value>
[&focus= <value>] - Focus operation</value>
[&iris= <value>] - Iris operation</value>
[&auto= <value>] - Auto pan, patrol</value>
[&zoom= <value>] - Zoom in, out</value>
[&zooming= <value>&zs=<value>] - Zoom without stopping, used for joystick</value></value>
[&vx= <value>&vy=<value>&vs=<value>] - Shift without stopping, used for joystick</value></value></value>
[&x= <value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] - Click on image</value></value></value></value></value>
(Move the center of image to the coordination (x,y) based on resolution or videosize.)
[[&speedpan= <value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>][&speedlink</value></value></value></value>
= <value>]] – Set speeds</value>
[&return= <return page="">]</return>

Example:

http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&move=right

http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&zoom=tele

http://myserver/cgi-bin/viewer/camctrl.cgi?channel=0&camid=1&x=300&y=200&resolution=704x480&vi deosize=704x480&strech=1

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
camid	0, <positive integer=""></positive>	Camera ID.
move	home	Move to camera to home position.
	up	Move camera up.
	down	Move camera down.
	left	Move camera left.
	right	Move camera right.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedfocus	-5 ~ 5	Set the focus speed.

speedapp	-5 ~ 5	Set the auto pan/patrol speed.
auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop camera.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
	stop	Stop zoom.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs
		speed, used for joystick control.
zs	0 ~ 6	Set the speed of zooming, "0" means stop.
	0~15 <sd81x1></sd81x1>	
vx	<integer ,="" 0="" excluding=""></integer>	The slope of movement = vy/vx , used for joystick control.
vy	<integer></integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.
	0 ~ 15 <sd81x1></sd81x1>	
x	<integer></integer>	x-coordinate clicked by user.
		It will be the x-coordinate of center after movement.
у	<integer></integer>	y-coordinate clicked by user.
		It will be the y-coordinate of center after movement.
videosize	<window size=""></window>	The size of plug-in (ActiveX) window in web page
resolution	<window size=""></window>	The resolution of streaming.
stretch	<boolean></boolean>	0 indicates that it uses resolution (streaming size) as the range
		of the coordinate system.
		1 indicates that it uses videosize (plug-in size) as the range of
		the coordinate system.
focus	auto	Auto focus.
	far	Focus on further distance.
	near	Focus on closer distance.
iris	auto	Let the Network Camera control iris size.
	open	Manually control the iris for bigger size.
	close	Manually control the iris for smaller size.
speedlink	0 ~ 4	Issue speed link command.
gaptime	0~32768	The gaptime between two consecutive ptz commands for device.
		(unit: ms)

return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the parameter is
		assigned. The < <i>return page</i> > can be a full URL path or relative
		path according to the current path. If you omit this parameter, it
		will redirect to an empty page.

8.10 ePTZ Camera Control (capability.eptz > 0, not used in

FE8174)

Note: This request requires camctrl privileges. **Method:** GET/POST

Method: GET/POS

Syntax:

http://< <i>servername</i> >/cgi-bin/camctrl/eCamCtrl.cgi?channel= <value>&stream=<value></value></value>
[&move= <value>] - Move home, up, down, left, right</value>
[&auto= <value>] - Auto pan, patrol</value>
[&zoom= <value>] - Zoom in, out</value>
[&zooming= <value>&zs=<value>] - Zoom without stopping, used for joystick</value></value>
[&vx= <value>&vy=<value>&vs=<value>] - Shift without stopping, used for joystick</value></value></value>
[&x= <value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] - Click on image</value></value></value></value></value>
(Move the center of image to the coordination (x,y) based on resolution or videosize.)
[[&speedpan= <value>][&speedtilt=<value>][&speedzoom=<value>][&speedapp=<value>]] - Set</value></value></value></value>
speeds
[&return= <return page="">]</return>

Example:

http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=0&move=right http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&vx=2&vy=2&vz=2 http://myserver/cgi-bin/camctrl/eCamCtrl.cgi?channel=0&stream=1&x=100&y=100& videosize=640x480&resolution=640x480&stretch=0

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
stream	<0~(m-1)>	Stream.
move	home	Move to home ROI.
	up	Move up.
	down	Move down.
	left	Move left.
	right	Move right.

auto	pan	Auto pan.
	patrol	Auto patrol.
	stop	Stop auto pan/patrol.
zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
zooming	wide or tele	Zoom without stopping for larger view or further view with zs speed, used for joystick control.
zs	0 ~ 6	Set the speed of zooming, "0" means stop.
vx	<integer></integer>	The direction of movement, used for joystick control.
vy	<integer></integer>	
vs	0 ~ 7	Set the speed of movement, "0" means stop.
x	<integer></integer>	x-coordinate clicked by user.
		It will be the x-coordinate of center after movement.
у	<integer></integer>	y-coordinate clicked by user.
		It will be the y-coordinate of center after movement.
videosize	<window size=""></window>	The size of plug-in (ActiveX) window in web page
resolution	<window size=""></window>	The resolution of streaming.
stretch	<boolean></boolean>	0 indicates that it uses resolution (streaming size) as the range
		of the coordinate system.
		1 indicates that it uses videosize (plug-in size) as the range of
		the coordinate system.
speedpan	-5 ~ 5	Set the pan speed.
speedtilt	-5 ~ 5	Set the tilt speed.
speedzoom	-5 ~ 5	Set the zoom speed.
speedapp	1 ~ 5	Set the auto pan/patrol speed.
return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the parameter is assigned. The < <i>return page</i> > can be a full URL path or relative path according to the current path.

8.11 Recall (capability.ptzenabled, not used in FE8174)

Note: This request requires Viewer privileges.

Method: GET

Syntax:

http://< <i>servername</i> >/cgi-bin/viewer/recall.cgi?
recall= <value>[&channel=<value>][&return=<<i>return page</i>>]</value></value>

PARAMETER	VALUE	DESCRIPTION
recall	Text string less than 30	One of the present positions to recall.
	characters	
channel	<0~(n-1)>	Channel of the video source.
return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the parameter is
		assigned. The < <i>return page</i> > can be a full URL path or relative
		path according to the current path. If you omit this parameter, it
		will redirect to an empty page.

8.12 ePTZ Recall (capability.eptz > 0, not used in FE8174)

Note: This request requires camctrl privileges.

Method: GET/POST

Syntax:

```
http://<servername>/cgi-bin/camctrl/eRecall.cgi?channel=<value>&stream=<value>&
recall=<value>[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.
recall	Text string less than 40	One of the present positions to recall.
	characters	
return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the parameter is
		assigned. The < <i>return page</i> > can be a full URL path or relative
		path according to the current path.

8.13 Preset Locations (capability.ptzenabled, not used in FE8174)

Note: This request requires Operator privileges. Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/preset.cgi?[channel=<value>] [&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
addpos	<text less="" string="" td="" than<=""><td>Add one preset location to the preset list.</td></text>	Add one preset location to the preset list.
	30 characters>	
channel	<0~(n-1)>	Channel of the video source.
delpos	<text less="" string="" td="" than<=""><td>Delete preset location from preset list.</td></text>	Delete preset location from preset list.
	30 characters>	
return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the parameter is
		assigned. The < <i>return page</i> > can be a full URL path or relative
		path according to the current path. If you omit this parameter, it
		will redirect to an empty page.

8.14 ePTZ Preset Locations (capability.eptz > 0, not used in

FE8174)

Note: This request requires Operator privileges. **Method:** GET/POST

Syntax:

http://<*servername*>/cgi-bin/operator/ePreset.cgi?channel=<value>&stream=<value> [&addpos=<value>][&delpos=<value>][&return=<*return page*>]

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of the video source.
stream	<0~(m-1)>	Stream.

addpos	<text less="" string="" th="" than<=""><th>Add one preset location to the preset list.</th></text>	Add one preset location to the preset list.
	40 characters>	
delpos	<text less="" string="" than<br="">40 characters></text>	Delete preset location from the preset list.
return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the parameter is assigned. The < <i>return page</i> > can be a full URL path or relative path according to the current path.

8.15 Fisheye local dewarp camera control (capability.

fisheyelocaldewarp.c0 > 0)

Note: This request requires camctrl privileges. **Method:** GET/POST

Syntax:

http:// <servername>/cgi-bin/camctrl/fdCamCtrl.cgi?channel=<value>&stream=<value></value></value></servername>
[&move= <value>] – Move home, up, down, left, right</value>
[&zoom= <value>] – Zoom wide, tele</value>
[[&speedpan= <value>][&speedtilt=<value>][&speedzoom=<value>]] - Set speeds</value></value></value>
[&x= <value>&y=<value>&videosize=<value>&resolution=<value>&stretch=<value>] - Click on image</value></value></value></value></value>
(Move the center of image to the coordination (x,y) based on resolution or videosize of 10 mode.)
[&return= <return page="">]</return>

Example:

http://myserver/cgi-bin/camctrl/fdCamCtrl.cgi?channel=0&stream=0&move=right http://myserver/cgi-bin/camctrl/fdCamCtrl.cgi?channel=0&stream=0&zoom=tele http://myserver/cgi-bin/camctrl/fdCamCtrl.cgi?channel=0&stream=0&move=top&speedtilt=-1 http://myserver/cgi-bin/camctrl/fdCamCtrl.cgi?channel=0&stream=0&x=700&y=700&videosize=1920x19 20&resolution=1920x1920&stretch=1

PARAMETER	VALUE	DESCRIPTION
channel	<0~(n-1)>	Channel of video source.
stream	<0~(m-1)>	Stream.
move	home	Move to home position.
	up	Move up.
	down	Move down.
	left	Move left.
	right	Move right.

zoom	wide	Zoom larger view with current speed.
	tele	Zoom further with current speed.
speedpan	-5 ~ 5	Set the pan speed of current command.
speedtilt	-5 ~ 5	Set the tilt speed of current command.
speedzoom	-5 ~ 5	Set the zoom speed of current command.
х	<integer></integer>	x-coordinate clicked by user.
		It will be the x-coordinate of center after movement.
У	<integer></integer>	y-coordinate clicked by user.
		It will be the y-coordinate of center after movement.
videosize	<window size=""></window>	The size of plug-in (ActiveX) window in web page of 10 content.
resolution	<window size=""></window>	The resolution of streaming of 10 content.
stretch	<boolean></boolean>	0 indicates that it uses resolution (streaming size) as the range
		of the coordinate system.
		1 indicates that it uses videosize (plug-in size) as the range of
		the coordinate system.
return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the parameter is
		assigned. The < <i>return page</i> > can be a full URL path or relative
		path according to the current path. If you omit this parameter, it
		will redirect to an empty page.

8.16 IP Filtering

Note: This request requires Administrator access privileges.

Method: GET/POST

Syntax: <product dependent>

http://<servername>/cgi-bin/admin/ipfilter.cgi?type[=<value>]

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=add<v4/v6>&ip=*<ipaddress*>[&index=<value>] [&return=<*return page*>]

http://<*servername*>/cgi-bin/admin/ipfilter.cgi?method=del<v4/v6>&index=<value>[&return=<*return* page>]

PARAMETER	VALUE	DESCRIPTION
type	NULL	Get IP filter type
	allow, deny	Set IP filter type
method	addv4	Add IPv4 address into access list.
	addv6	Add IPv6 address into access list.
	delv4	Delete IPv4 address from access list.

	delv6	Delete IPv6 address from access list.
ір	<ip address=""></ip>	Single address: <ip address=""></ip>
		Network address: <ip address="" mask="" network=""></ip>
		Range address: <start -="" address="" end="" ip=""></start>
index	<value></value>	The start position to add or to delete.
return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the parameter is
		assigned. The < <i>return page</i> > can be a full URL path or relative
		path according to the current path. If you omit this parameter, it
		will redirect to an empty page.

8.17 UART HTTP Tunnel Channel (capability.nuart > 0)

Note: This request requires Operator privileges.

Method: GET and POST

Syntax:

http:// <servername>/cgi-bin/operator/uartchannel.cgi?[channel=<value>]</value></servername>
GET /cgi-bin/operator/uartchannel.cgi?[channel= <value>]</value>
x-sessioncookie: string[22]
accept: application/x-vvtk-tunnelled
pragma: no-cache
cache-control: no-cache
POST /cgi-bin/operator/uartchannel.cgi
x-sessioncookie: string[22]
content-type: application/x-vvtk-tunnelled
pragma : no-cache
cache-control : no-cache
content-length: 32767
expires: Sun, 9 Jam 1972 00:00:00 GMT

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through a proxy server.

This channel will help to transfer the raw data of UART over the network. Please see UART tunnel spec for detail information

PARAMETER	VALUE	DESCRIPTION
channel	0 ~ (n-1)	The channel number of UART.

8.18 Event/Control HTTP Tunnel Channel (capability.

evctrlchannel > 0)

Note: This request requires Administrator privileges.

Method: GET and POST

Syntax:

User must use GET and POST to establish two channels for downstream and upstream. The x-sessioncookie in GET and POST should be the same to be recognized as a pair for one session. The contents of upstream should be base64 encoded to be able to pass through the proxy server.

This channel will help perform real-time event subscription and notification as well as camera control more efficiently. The event and control formats are described in another document.

See Event/control tunnel spec for detail information

8.19 Get SDP of Streams

Note: This request requires Viewer access privileges. **Method:** GET/POST

Syntax:

http://<servername>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

"network_accessname_<0~(m-1)>" is the accessname for stream "1" to stream "m". Please refer to the

"subgroup of network: rtsp" for setting the accessname of SDP.

You can get the SDP by HTTP GET.

When using scalable multicast, Get SDP file which contains the multicast information via HTTP.

8.20 Open the Network Stream

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://<*servername*>/<network_http_s<0~m-1>_accessname>

For RTSP (MP4), the user needs to input the URL below into an RTSP compatible player.

rtsp://<servername>/<network_rtsp_s<0~m-1>_accessname>

"m" is the stream number.

For details on streaming protocol, please refer to the "control signaling" and "data format" documents.

8.21 Senddata (capability.nuart > 0)

Note: This request requires Viewer privileges. Method: GET/POST

Syntax:

http://<*servername*>/cgi-bin/viewer/senddata.cgi? [com=<value>][&data=<value>][&flush=<value>] [&wait=<value>] [&read=<value>]

PARAMETER	VALUE	DESCRIPTION
com	1 ~ <max. com="" port<="" td=""><td>The target COM/RS485 port number.</td></max.>	The target COM/RS485 port number.
	number>	
data	<hex decimal<="" td=""><td>The <hex data="" decimal=""> is a series of digits from 0 \sim 9, A \sim F.</hex></td></hex>	The <hex data="" decimal=""> is a series of digits from 0 \sim 9, A \sim F.</hex>
	data>[, <hex decimal<="" td=""><td>Each comma separates the commands by 200 milliseconds.</td></hex>	Each comma separates the commands by 200 milliseconds.
	data>]	
flush	yes,no	yes: Receive data buffer of the COM port will be cleared before
		read.
		no: Do not clear the receive data buffer.
wait	1 ~ 65535	Wait time in milliseconds before read data.
read	1 ~ 128	The data length in bytes to read. The read data will be in the
		return page.

Return:

HTTP/1.0 200 OK\r\n Content-Type: text/plain\r\n Content-Length: <system information length>\r\n \r\n <hex decimal data>\r\n

Where hexadecimal data is digits from 0 \sim 9, A \sim F.

8.22 Storage managements (capability.storage.dbenabled > 0)

Note: This request requires administrator privileges.

Method: GET and POST

Syntax:

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=<cmd_type>[&<parameter>=<value>...]

The commands usage and their input arguments are as follows.

PARAMETER	VALUE	DESCRIPTION
cmd_type	<string></string>	Required.
		Command to be executed, including search, insert, delete,
		update, and queryStatus.

Command: search

PARAMETER	VALUE	DESCRIPTION
label	<integer key="" primary=""></integer>	Optional.
		The integer primary key column will automatically be assigned
		a unique integer.
triggerType	<text></text>	Optional.
		Indicate the event trigger type.
		Please embrace your input value with single quotes.
		Ex. mediaType='motion'
		Support trigger types are product dependent.
mediaType	<text></text>	Optional.
		Indicate the file media type.
		Please embrace your input value with single quotes.
		Ex. mediaType='videoclip'
		Support trigger types are product dependent.
destPath	<text></text>	Optional.
		Indicate the file location in camera.
		Please embrace your input value with single quotes.
		Ex. destPath ='/mnt/auto/CF/NCMF/abc.mp4'
resolution	<text></text>	Optional.
		Indicate the media file resolution.
		Please embrace your input value with single quotes.
		Ex. resolution='800x600'
isLocked	<boolean></boolean>	Optional.

216 - User's Manual

		Indicate if the file is locked or not.		
		0: file is not locked.		
		1: file is locked.		
		A locked file would not be removed from UI or cyclic storage.		
triggerTime	<text></text>	Optional.		
		Indicate the event trigger time. (not the file created time)		
		Format is "YYYY-MM-DD HH:MM:SS"		
		Please embrace your input value with single quotes.		
		Ex. triggerTime='2008-01-01 00:00:00'		
		If you want to search for a time period, please apply "TO"		
		operation.		
		Ex. triggerTime='2008-01-01 00:00:00'+TO+'2008-01-01		
		23:59:59' is to search for records from the start of Jan 1^{st} 2008		
		to the end of Jan 1 st 2008.		
limit	<positive integer=""></positive>	Optional.		
		Limit the maximum number of returned search records.		
offset	<positive integer=""></positive>	Optional.		
		Specifies how many rows to skip at the beginning of the		
		matched records.		
		Note that the offset keyword is used after limit keyword.		

To increase the flexibility of search command, you may use "OR" connectors for logical "OR" search operations. Moreover, to search for a specific time period, you can use "TO" connector.

Ex. To search records triggered by motion or di or sequential and also triggered between 2008-01-01 00:00:00 and 2008-01-01 23:59:59.

http://<*servername*>/cgi-bin/admin/lsctrl.cgi?cmd=search&triggerType='motion'+OR+'di'+OR+'seq'&trigge rTime='2008-01-01 00:00:00'+TO+'2008-01-01 23:59:59'

Command: **delete**

PARAMETER	VALUE	DESCRIPTION	
label	<integer key="" primary=""></integer>	Required.	
		Identify the designated record.	
		Ex. label=1	

Ex. Delete records whose key numbers are 1, 4, and 8.

http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=delete&label=1&label=4&label=8

Command: update

PARAMETER	VALUE	DESCRIPTION

label	<integer key="" primary=""></integer>	Required.	
		Identify the designated record.	
		Ex. label=1	
isLocked	<boolean></boolean>	Required.	
		Indicate if the file is locked or not.	

Ex. Update records whose key numbers are 1 and 5 to be locked status.

http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=1&label=1&label=5

Ex. Update records whose key numbers are 2 and 3 to be unlocked status.

```
http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=update&isLocked=0&label=2&label=3
```

Command: queryStatus

PARAMETER	VALUE	DESCRIPTION	
retType	xml or javascript	Optional.	
		Ex. retype=javascript	
		The default return message is in XML format.	

Ex. Query local storage status and call for javascript format return message.

http://<servername>/cgi-bin/admin/lsctrl.cgi?cmd=queryStatus&retType=javascript

8.23 Virtual input (capability.nvi > 0)

Note: Change virtual input (manual trigger) status.

Method: GET

Syntax:

```
http://<servername>/cgi-bin/admin/setvi.cgi?vi0=<value>[&vi1=<value>][&vi2=<value>]
[&return=<return page>]
```

PARAMETER	VALUE	DESCRIPTION
vi <num></num>	state[(duration)nstate]	Ex: vi0=1
		Setting virtual input 0 to trigger state
	Where "state" is 0, 1. "0"	
	means inactive or normal	Ex: vi0=0(200)1
	state while "1" means	Setting virtual input 0 to normal state, waiting 200
	active or triggered state.	milliseconds, setting it to trigger state.
	Where "nstate" is next	Note that when the virtual input is waiting for next state,

	state after duration.	it cannot accept new requests.
return	<return page=""></return>	Redirect to the page < <i>return page</i> > after the request is completely assigned. The < <i>return page</i> > can be a full URL path or relative path according the current path. If you omit this parameter, it will redirect to an empty page.

Return Code	Description	
200	The request is successfully executed.	
400	The request cannot be assigned, ex. incorrect parameters.	
	Examples:	
	setvi.cgi?vi0=0(10000)1(15000)0(20000)1	
	No multiple duration.	
	setvi.cgi?vi3=0	
	VI index is out of range.	
	setvi.cgi?vi=1	
	No VI index is specified.	
503	The resource is unavailable, ex. Virtual input is waiting for next state.	
	Examples:	
	setvi.cgi?vi0=0(15000)1	
	setvi.cgi?vi0=1	
	Request 2 will not be accepted during the execution time(15 seconds).	

8.24 Open Timeshift Stream (capability.timeshift > 0,

timeshift_enable=1, timeshift_c<n>_s<m>_allow=1)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

```
http://<servername>/<network_http_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime
=<value>&forcechk&minsft=<value>]
```

For RTSP (MP4 and H264), the user needs to input the URL below into an RTSP compatible player.

```
rtsp://<servername>/<network_rtsp_s<m>_accessname>?maxsft=<value>[&tsmode=<value>&reftime
=<value>&forcechk&minsft=<value>]
```

"n" is the channel index.

"m" is the timeshift stream index.

For details on timeshift stream, please refer to the "TimeshiftCaching" documents.

PARAMETER	VALUE	DEFAULT	DESCRIPTION	
maxsft	<positive< td=""><td>0</td><td>Request cached stream at most how many seconds ago.</td></positive<>	0	Request cached stream at most how many seconds ago.	
	interger>			
tsmode	normal,	normal	Streaming mode:	
	adaptive		normal => Full FPS all the time.	
			adaptive => Default send only I-frame for MP4 and	
			H.264, and send 1 FPS for MJPEG. If DI or motion window	
			are triggered, the streaming is changed to send full FPS	
			for 10 seconds.	
			(*Note: this parameter also works on non-timeshift	
			streams.)	
reftime	mm:ss	The time	Reference time for maxsft and minsft.	
		camera receives	(This provides more precise time control to eliminate the	
		the request.	inaccuracy due to network latency.)	
			Ex: Request the streaming from 12:20	
			rtsp://10.0.0.1/live.sdp?maxsft=10&reftime=12:30	
forcechk	N/A	N/A	Check if the requested stream enables timeshift, feature	
			and if minsft is achievable.	
			If false, return "415 Unsupported Media Type".	
minsft	<positive< td=""><td>0</td><td>How many seconds of cached stream client can accept at</td></positive<>	0	How many seconds of cached stream client can accept at	
	interger>		least.	
			(Used by forcechk)	

Return Code	Description	
400 Bad Request	Request is rejected because some parameter values are illegal.	
415 Unsupported Media Type	Returned, if forcechk appears, when minsft is not achievable or the	
	timeshift feature of the target stream is not enabled.	

8. 25 Open Anystream (capability.nanystream > 0)

Note: This request requires Viewer access privileges.

Syntax:

For HTTP push server (MJPEG):

http://<servername>/videoany.mjpg?codectype=mjpeg[&resolution=<value>&mjpeg_quant=<value>& mjpeg_qvalue=<value>&mjpeg_maxframe=<value>]

For RTSP (MPEG4), the user needs to input the URL below into an RTSP compatible player.

rtsp://<servername>/liveany.sdp?codectype=mpeg4[&resolution=<value>&mpeg4_intraperiod=<value> &mpeg4_ratecontrolmode=<value>&mpeg4_quant=<value>&mpeg4_qvalue=<value>&mpeg4_bitrate= <value>&mpeg4_maxframe=<value>]

For RTSP (H264), the user needs to input the URL below into an RTSP compatible player.

rtsp://<servername>/liveany.sdp?codectype=h264[&resolution=<value>&h264_intraperiod=<value>&

h264_ratecontrolmode=<value>& h264_quant=<value>& h264_qvalue=<value>&

h264_bitrate=<value>& h264_maxframe=<value>]

<product dependent>

PARAMETER	VALUE	DEFAULT	DESCRIPTION
codectype	mjpeg, mpeg4, h264	N/A	Set codec type for Anystream.
	<product dependent=""></product>		
solution	capability_videoin_resolution	<product< td=""><td>Video resolution in pixels.</td></product<>	Video resolution in pixels.
		dependent>	
mjpeg_quant	0, 1~5	3	Quality of JPEG video.
	99, 1~5		0,99 is the customized manual input
	<product dependent=""></product>		setting.
			1 = worst quality, 5 = best quality.
			<product dependent=""></product>
mjpeg_qvalue	10~200	50	Manual video quality level input.
	2~97	<product< td=""><td>(This must be present if mjpeg_quant</td></product<>	(This must be present if mjpeg_quant
	<product dependent=""></product>	dependent>	is equal to 0, 99)
			<product dependent=""></product>
mjpeg_maxframe	1~25,	15	Set maximum frame rate in fps (for
	26~30 (only for NTSC or		JPEG).
	60Hz CMOS)		
mpeg4_intraperiod	250, 500, 1000, 2000, 3000,	1000	Intra frame period in milliseconds.
	4000		

mpeg4_ratecontrolmode	cbr. vbr	vbr	cbr: constant bitrate
			vbr: fix quality
mpeg4_quant	0, 1~5	3	Quality of video when choosing vbr in
	99, 1~5		"mpeg4_ratecontrolmode".
	<product dependent=""></product>		0,99 is the customized manual input
			setting.
			1 = worst quality, 5 = best quality.
			<pre><pre><pre><pre><pre><pre><pre><pre></pre></pre></pre></pre></pre></pre></pre></pre>
mpeg4_qvalue	1~31	7	Manual video quality level input.
	2~31	<product< td=""><td>(This must be present if mpeg4_quant</td></product<>	(This must be present if mpeg4_quant
	<product dependent=""></product>	dependent>	is equal to 0, 99)
	F		<pre><pre>product dependent></pre></pre>
			<pre><pre>cproduct dependent></pre></pre>
mpeg4_bitrate	1000~8000000	512000	Set bit rate in bps when choosing cbr
	1000~4000000	<product< td=""><td>in "mpeg4_ratecontrolmode".</td></product<>	in "mpeg4_ratecontrolmode".
	<product dependent=""></product>	dependent>	
mpeg4_maxframe	1~25,	10	Set maximum frame rate in fps (for
	26~30 (only for NTSC or	15	MPEG-4).
	60Hz CMOS)	<product< td=""><td></td></product<>	
	,	dependent>	
h264_intraperiod	250, 500, 1000, 2000, 3000,	1000	Intra frame period in milliseconds.
	4000		
h264_ratecontrolmode	cbr, vbr	vbr	cbr: constant bitrate
			vbr: fix quality
h264_quant	0, 1~5	3	Quality of video when choosing vbr in
	99, 1~5		"h264_ratecontrolmode".
	<product dependent=""></product>		0,99 is the customized manual input
			setting.
			1 = worst quality, 5 = best quality.
			<product dependent=""></product>
h264_qvalue	0~51	30	Manual video quality level input.
	<product dependent=""></product>	<product< td=""><td>(This must be present if h264_quant is</td></product<>	(This must be present if h264_quant is
		dependent>	equal to 0, 99)
			<product dependent=""></product>
h264_bitrate	1000~8000000	512000	Set bit rate in bps when choosing cbr
	1000~4000000	<product< td=""><td>in "h264_ratecontrolmode".</td></product<>	in "h264_ratecontrolmode".
	<product dependent=""></product>	dependent>	
h264_maxframe	1~25,	10	Set maximum frame rate in fps (for
	26~30 (only for NTSC or	15	H264).
	60Hz CMOS)	<product< td=""><td></td></product<>	

	dependent>
--	------------

8.26 Export Files

Note: This request requires Administrator privileges.

Method: GET

Syntax:

For daylight saving time configuration file:

http://<*servername*>/cgi-bin/admin/exportDst.cgi

For language file:

http://<servername>/cgi-bin/admin/export_language.cgi?currentlanguage=<value>

PARAMETER	VALUE	DESCRIPTION	
currentlanguage	0~20	Available language lists.	
		Please refer to:	
		system_info_language_i0 ~ system_info_language_i19.	

For setting backup file:

http://<servername>/cgi-bin/admin/export_backup.cgi?backup

8.27 Upload Files

Note: This request requires Administrator privileges.

Method: POST

Syntax:

For daylight saving time configuration file:

http://<*servername*>/cgi-bin/admin/upload_dst.cgi

Post data:

filename =<file name>\r\n

\r\n

<multipart encoded form data>

For language file:

http://<*servername*>/cgi-bin/admin/upload_lan.cgi

Post data:

filename =<file name>\r\n \r\n <multipart encoded form data>

For setting backup file:

http://<servername>/cgi-bin/admin/upload_backup.cgi

Post data:

filename =<file name>\r\n \r\n <multipart encoded form data>

Server will accept the file named <file name> to upload this one to camera.

8.28 Media on demand

Media on demand allows users to select and receive/watch/listen to metadata/video/audio contents on demand.

Note: This request requires Viewer access privileges.

Syntax:

rtsp://<servername>/mod.sdp?[&stime=<value>][&etime=<value>][&length =<value>][&loctime =<value>][&file=<value>][&tsmode=<value>]

PARAMETER	VALUE	DEFAULT	DESCRIPTION	
stime	<yyyymmdd_hhmmss.mmm></yyyymmdd_hhmmss.mmm>	N/A	Start time.	
etime	<yyyymmdd_hhmmss.mmm></yyyymmdd_hhmmss.mmm>	N/A	End time.	
length	<positive integer=""></positive>	N/A	The length of media of interest.	
			The unit is second.	
loctime	octime <boolean> 0</boolean>		Specify if start/end time is local time format	
			1 for local time, 0 for UTC+0	
file	<string></string>	N/A	The media file to be played.	
tsmode	<positive integer=""></positive>	N/A	Timeshift mode, the unit is second.	

Ex.

stime	etime	length	file	Description	
V	V	Х	Х	Play recordings between stime and etime	
				rtsp://10.10.1.2/mod.sdp?stime=20110312_040400.000	
				&etime=2011_0312_040510.000	
V	Х	V	Х	Play recordings for <code>length</code> seconds which start from <code>stime</code>	
				rtsp://10.10.1.2/mod.sdp?stime=20110312_040400.000	

				&length=120
Х	V	V	Х	Play recordings for length seconds which ends at etime
				rtsp://10.10.1.2/mod.sdp?etime=20110312_040400.000
				&length=120
Х	Х	Х	V	Play file file
				rtsp://10.10.1.2/mod.sdp?filename=/mnt/link0/

<End of document>

Technical Specifications

Technical Specifications

Models	EE8174/74\/	Alarm and Event	
Models	FE8174/74V	Alarm Triggers	Video motion detection, manual trigger, digital input, periodical
System Information		Addit Higgers	trigger, system boot, recording notification, camera tampering detection
CPU	Multimedia SoC (System-on-Chip)	Alarm Events	Event notification using digital output, HTTP, SMTP, FTP and
Flash RAM	128 MB 256 MB		NAS server
	230 MB		File upload via HTTP, SMTP, FTP and NAS server
Camera Features		General	
Image Sensor	1/2.5" Progressive CMOS in 2560 x 1920 resolution	Connectors	RJ-45 cable connector for Network/PoE connection
Maximum Resolution	1920x1920		Audio input
Lens Type	Fixed-focal		Audio output DC 12V power input
Focal Length	f = 1.5 mm		Digital input*1
Aperture	F2.8		Digital output*1
Field of View	180° (Horizontal)	LED Indicator	System power and status indicator
	180° (Vertical)	Power Input	DC 12V
Shutter Time	180° (Diagonal)	Device Consumption	IEEE 802.3af PoE Class 2
	1/5 sec. to 1/32,000 sec. WDR Enhanced	Power Consumption	Max. 5.1 W (DC 12V) Max 5.3 W (PoE)
WDR Technology Day/Night	Removable IR-cut filter for day & night function	Dimensions	Ø: 145 mm x 47 mm (FE8174V)
Minimum Illumination	0.03 Lux @ F2.8, 50 IRE (Color)		Ø: 139 mm x 34 mm (FE8174)
	0.001 Lux @ F2.8, 50 IRE (B/W)	Weight	Net: 545 g (FE8174V)
Pan/tilt/zoom Functionalities	ePTZ:	Casting	Net: 358 g (FE8174)
	12x digital zoom (12x on IE plug-in)	Casing	Vandal-proof IK10-rated metal housing (FE8174V) Weather-proof IP66-rated housing (FE8174V)
On-board Storage	MicroSD/SDHC/SDXC card slot	Safety Certifications	CE, LVD, FCC Class A, VCCI, C-Tick, EN50155 (FE8174V), UL
Video		Operating Temperature	Starting Temperature: -25°C ~ 50°C (-13°F ~ 122°F)
VIGEO			Working Temperature: -40°C ~ 50°C (-40°F ~ 122°F)
Compression	H.264, MJPEG & MPEG-4	Warranty	36 months
Maximum Frame Rate	15 fps at 1920x1920	System Requirements	
	30 fps at 1920x1080	Operating System	Microsoft Windows 7/Vista/XP/2000
	In all compression modes	Web Browser	Mozilla Firefox 7~10 (Streaming only)
Maximum Streams	3 simultaneous streams		Internet Explorer 7/8/9
S/N Ratio Dynamic Range	Above 62 dB 57 dB	Other Players	VLC: 1.1.11 or above Quicktime: 7 or above
Video Streaming	Adjustable resolution, quality and bitrate		Quicklime. 7 or above
Image Settings	Adjustable image size, quality and bit rate	Included Accessories	
initigo ootanigo	Pixel counter	CD	User's manual, quick installation guide, Installation Wizard 2,
	Time stamp, text overlay, flip & mirror		ST7501 32-channel recording software
	Configurable brightness, contrast, saturation, sharpness, wh	Others	Quick installation guide, warranty card, alignment sticker, desiccant bag, screw driver, screws pack, I/O cable, mounting
	balance, exposure control, gain, backlight compensation, pri	vacy	bracket, software CD
	masks		
	Scheduled profile settings	Dimonsions	
Audio		Dimensions	
Audio Capability	Audio input/output (full duplex)		
Compression	AAC, G.711, G.726	• FE8174V	• FE8174
Interface	Built-in microphone		× T ~ ~
	External microphone input		
Effective Range	5 meters		
Network			
Users	Live viewing for up to 10 clients		//// 15 (\ 🔍 // 19
Protocols	IPv4, IPv6, TCP/IP, HTTP, HTTPS, UPnP, RTSP/RTP/RTC		
	IGMP, SMTP, FTP, DHCP, NTP, DNS, DDNS, PPPoE, Cos		
Interface	QoS, SNMP, 802.1X, UDP, ICMP		
	10Base-T/100 BaseTX Ethernet (RJ-45)		
ONVIF	Supported, specification available at www.onvif.org		
Intelligent Video		n n	
Video Motion Detection	Five-window video motion detection		
Compatible Acce	essories		
Mounting Kits		Power Adapter	PoE Kits
AM-518 Dome adapter	AM-114 Pendant head	AA-221 DC 12V Power Adapter	POE-IJ-1748NDN PoE injector, 802.3af compliant
		0	Alle.



Distributed by:

AM-515

NPT adapter (for AM-518)



Technology License Notice

MPEG-4 AAC Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 AAC AUDIO PATENT LICENSE. THIS PRODUCT MAY NOT BE DECOMPILED, REVERSE-ENGINEERED OR COPIED, EXCEPT WITH REGARD TO PC SOFTWARE, OF WHICH YOU MAY MAKE SINGLE COPIES FOR ARCHIVAL PURPOSES. FOR MORE INFORMATION, PLEASE REFER TO <u>HTTP://WWW.VIALICENSING.COM</u>.

MPEG-4 Visual Technology

THIS PRODUCT IS LICENSED UNDER THE MPEG-4 VISUAL PATENT PORTFOLIO LICENSE FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER FOR (i) ENCODING VIDEO IN COMPLIANCE WITH THE MPEG-4 VISUAL STANDARD ("MPEG-4 VIDEO") AND/OR (ii) DECODING MPEG-4 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/ OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED BY MPEG LA TO PROVIDE MPEG-4 VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION INCLUDING THAT RELATING TO PROMOTIONAL, INTERNAL AND COMMERCIAL USES AND LICENSING MAY BE OBTAINED FROM MPEG LA, LLC. PLEASE REFER TO <u>HTTP://WWW.MPEGLA.COM</u>.

AMR-NB Standard

THIS PRODUCT IS LICENSED UNDER THE AMR-NB STANDARD PATENT LICENSE AGREEMENT. WITH RESPECT TO THE USE OF THIS PRODUCT, THE FOLLOWING LICENSORS' PATENTS MAY APPLY:

TELEFONAKIEBOLAGET ERICSSON AB: US PAT. 6192335; 6275798; 6029125; 6424938; 6058359. NOKIA CORPORATION: US PAT. 5946651; 6199035. VOICEAGE CORPORATION: AT PAT. 0516621; BE PAT. 0516621; CA PAT. 2010830; CH PAT. 0516621; DE PAT. 0516621; DK PAT. 0516621; ES PAT. 0516621; FR PAT. 0516621; GB PAT. 0516621; GR PAT. 0516621; IT PAT. 0516621; LI PAT. 0516621; LU PAT. 0516621; NL PAT. 0516621; SE PAT 0516621; US PAT 5444816; AT PAT. 819303/AT E 198805T1; AU PAT. 697256; BE PAT. 819303; BR PAT. 9604838-7; CA PAT. 2216315; CH PAT. 819303; CN PAT. ZL96193827.7; DE PAT. 819303/DE69611607T2; DK PAT. 819303; ES PAT. 819303; EP PAT. 819303; FR PAT. 819303; GB PAT. 819303; IT PAT. 819303; JP PAT. APP. 8-529817; NL PAT. 819303; SE PAT. 819303; US PAT. 5664053. THE LIST MAY BE UPDATED FROM TIME TO TIME BY LICENSORS AND A CURRENT VERSION OF WHICH IS AVAILABLE ON LICENSOR'S WEBSITE AT HTTP://WWW.VOICEAGE.COM.

Electromagnetic Compatibility (EMC)

FCC Statement

This device compiles with FCC Rules Part 15. Operation is subject to the following two conditions.

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

VCCI Warning

この装置は、情報処理装置等電波障害自主規制協議会(VCCI)の基準にづくクラスB情報技術装置です。この 装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使 用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい

Liability

VIVOTEK Inc. cannot be held responsible for any technical or typographical errors and reserves the right to make changes to the product and manuals without prior notice. VIVOTEK Inc. makes no warranty of any kind with regard to the material contained within this document, including, but not limited to, the implied warranties of merchantability and fitness for any particular purpose.