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.

Nethod:	Create certificate request and install	
Country	TW	
State or province:	Asia Asia WVOTEK Inc.	
Locality.		
Organization:		
Organization unit	VIVOTEK Inc.	
Common name:	www.styplek.com	

4. The Certificate request window will prompt.

putb:0.180	1884 15 Deet of recursive and request the d - Wallows Intern. 16-186-18
COMICO	anone ordens controled
Copy the R By dicking 1	W fermat request below and earch 2 to a CA for dar6fy validation. After that, you have to instal te "Epicad" feature on HTTPR page
Ontheat	request (PEM Tormal)
	IN CENTIFICATE REQUEST
MITHERSON	AbuChgInouElMBAGALUIEBNACVFuuDTALSqFUBAqTSEFunResPCALAqAT
BACTELES	ANEXFIATEGRIFAATEFZIVESURINGSHIGTSICABUSALEESHOFFIAFIA
NAME AND ADDRESS OF	under all and a second s
SCAD4115	IIIIIboll0AL675_b_bLCoufOlg416080egEEbQ8aL64827baevbpon/4
ND2-JAIRE	MLQv9pepatty3cx07eu12u97bxb3Auftr/137Rdv04100x9ven3Ap1016
Spedica DV	VLD # VTnivusi z cenveli LYROWCLIEFL a dDUVERsCOVEgHLERG-76z 7+ MGLQKB
AAGgADAS	yoxdarraevoardii.yyoyoddarddarddaruuraevuuraevoargaraevoarga.
NB/Lg2TE	JCxPRENCALGS #J4XpPH5HVW0W0Lv0000/ssRERcSel#JtEIN1#JRDIALPH
TRANSFE IN	<pre>/C461#D0/Sbqf Se011867110C1p#INex8uTqFEHM77ysRgd#sseQu187s</pre>
SMagrflo	pine .
	CERCIFICALE 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.



6. 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 650.426.5112 option 3 or send an email to internet-sales@verisign.com
Thank you for your interest in Symantec!
BEGIN CERTIFICATE
MIIFBDCCA+ygAwIBAgIQFx1Cahn/SeBSit0WQDOBIzANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDl21cmlTaWduLCBJbmMuMTAwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAsTOVR1cm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc21nbi5jb20vY3Bz
L3Rlc3RjYSAoYykwOTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJ11FN1
cnZlciBDQSAtIEcyMB4XDTEyMDcwMzAwMDAwMFoXDTEyMDgwMjIzNTk10Vowga4x
CzAJBgNVBAYTA1RXMQ0wCwYDVQQ1EwRBc21hMQ0wCwYDVQQHFARBc21hMRUwEwYD
VQQKFAxWSVZPVEVLIEluYy4xFTATBgNVBAsUDFZJVk9URUsgSW5jLjE6MDgGA1UE
CxQxVGVybXMgb2YgdXNlIGF0IHd3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYSAo
YykwNTEXMBUGA1UEAxQOd3d3LmZ10DE3M15jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANiIE0tr8KGfcC+hA9UYFvg8XZCyTS3a72tunRyLKpdlid6eQ0dR
p/h+ajhtpTUQg5C7IWwxUBBCPFp/Q4xIPBoQpWUq50Z0GR/qgimARKjlxsxkPN/R
WxlIK5n1zwbloCDygrFEzRSCMQv945GDrEbRSkNuoMpqAhXo0Ko0nqqTAgMBAAGj
ggGBMI1BfTAZBgNVHREEEjAQgg53d3cuZmU4MTcyImNvbTAJBgNVHRMEAjAAMA4G
A1UdDwEB/wQEAwIFoDBDBgNVHR8EPDA6MDigNqA0hjJodHRw0i8vU12SVHJpYWwt
RzItY3JsLnZ1cmlzaWduLmNvbS9TV1JUcmlhbEcyLmNybDBKBgNVHSAEQzBBMD8G
CmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24u
Y29tL2Nwcy90ZXN0Y2EwHQYDVR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8G
A1UdIwQYMBaAFCgXE4q91qK13AYst7aO2hBmYG71MHQGCCsGAQUFBwEBBGgwZjAk
BggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVyaXNp224uY29tMD4GCCsGAQUFBzAC
hjJodHRwOi8vU12SVHJpYWwtRzItYWlhLnZlcmlzaWduLmNvbS9TVlJUcmlhbEcy
LmNlcjANBgkqhkiG9w0BAQUFAAOCAQEATxuH7FnIae/X7T6z/zzr9zEKhLKSEQSp
qaNc8swixSc129Pp3kzEKvp6TCLPSMbr0PGjPa1LFxAEUITr3WlSCoXWRlAjWp12
qVSbDfxgVMWx9T7rd2oURzjms6ifcM5Ttub3Qc2Tu3pWeAKbAH/U+x+ojG0EvB3z
cPaShn/qcapKcq0XvHycwHeCWN8RQgsGci368qkPzssv7oErbnLhupjdxUESGExu
3Ml3CXrAtQZv1Rad1fJQYSTgS0Nq2mA9ghdEuKTnhCHUwwqOxN8uceII83ITPK70
m6CoYpntb1gmFtyj9EvgIUdc6YZImn2B0qSc5q3iZARPH/gi//XeGg==
END CERTIFICATE

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



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

0	EARCH) - ORGANIS			. (0) ×1
Fle	Edt Search Inset Prop	ect May Po	Colars Marre Scription Advanced Window Help	
0	Open	Chi+li		哈爾隆 新用用用 白田 格 (4)
	Opera	Chi+0		an and a second second second second
12	quick open	CD#+0		* 8 8 5
12	Q004		1	
10	Cose Al (Nes	1011-35-01-45		0
L	Goss All Files Except This			ALC N
	PIETRINE.			S
	and the second second		BEAUGTEOR DA OWELLAN DOUGE DOE FREEN ANT FOREDO BEELYS I GU GUDAN E CERNENNE TIME VERMENTURE I REVIER AT THATED OFFICE AT DC CARA	7942592240
1	Terraria series		LIVERBARCHIZE 109 108 13475CTRCZNSW7071RHQ5CC80403F30	SEPORAL NET CODES
4	Ente .	Chi+i	bgEfBQcsANThaBBOcDovL29jc3AudaUyaDNpZ24uf29tBD49CC	A GAQUFTING
10	3040.85	9 <u>1</u> 2	NUMBER OF BADD 238 A PART & STEAM TUTUTUS TO ME 29 MORT 2010 10 MARK 88 LA T	JOGWINI KOS
-8	Save AF	49-1912	LeyAlBgieghei GSwill AGUF AROCAGEA Tei H7Fn Ian/ 1775 2/ 22292	CKBL#SEQ5p
12	200120123740		a Dit you'll a STIT of a Thirt in a fit for NS To up 1 Or 2 To 1 a Bail Thank Bail	eo100Evfla
12	Make Copy@acku#		Rha,/qnapEnq02vEyouReCMBREQgeCoi%68qlcPdaev?oIcbnlhap	auttenden 2
	Exception		CIr ht QDv1Fad1f3Q78Tg8CNg3mkSghdEvKTnhCHDewg0eMisce	11873778170
-	Parana Ma		aYynthigaFtyj9EvgTUdo6V21an2EGgBoSqDi2ADP#/gi//EeGg	
	Contains	164211	THE CENTERICALE	
1	Couport.	HITCH		
-	20	_	the last sector and	
	Cawaran		A Deriver a rec	15
	-sherm (Annous		- Destroye	3
현	5R.	C09+*	C. Contraction	
判	所統 得 Noo		3 BOICPERI	
14	Prat Prevent		AND	
	Prat Setup/Carliguation		Children Jageli	
10	Pojorite Piles .	COHORD IF	Attal to Gen Dover User	
	⊐ecent Mez		AbCII to Ungets	
	Recent Wotesta (Wotgspace)		· TTT & by groups	
10	S.0.		A LOUIS AND A LOUI	
			A BACCARDO M/CHINEN	

5	nc As				1	1 201
- 8 X	Sana in	Dieskrop		201		
tipe: Control (Links) tip: A tip: A tip: Control (Links) tip:	No Concepto	Mile Documento Mile Documento Mile Computer Mile	s a band 2 ky Scan Pha seart Grant Clarkt ret	UthusCorpare UthusCorpare WithusCost RedoceMP(2) 44 9745 9745 9745 9745 9745 9745 9745 9	Fighter of the dataset	4) 01 01
	Hy Unice	Fienane	CAUER OT		<u>r</u>] Seve	1
	AAAAA A	Save sutype	Al Res (**)		Earcel	
		Line Territotor:	Default		*	1
que vertue		Feme:	Detect		*	
			Labor of Delayer to	prorystian acidariae)	1	
		405 Stream	-			
			OP-Date Street Service	O'DER MARK NUMBER		

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.

			Home	Client settings	Configuration	Language
	Security	/ > HTTPS		-		
System	- HTTP	S				
Media	🔽 En	able HTTPS secure connecti	on			
Network	₩ Mo	de:				
Security		⊙ HTTP & HTTPS ○ HTT	TPS only			
User accounts	🐨 Ce	rtificate:				
HTTPS		Certificate information				
Access list		Status:	Waiti	ng for certificated		
IEEE 802.1x		Select certificate file:	C:\D	ocuments and Se	rowse Upload	
РТΖ		Method:	Creat	te certificate request a	ind install	
Event		Country:	TW			
Applications		State or province:	Asia			
		Locality:	Asia			
Recording		Organization:	VIVO	TEK Inc.		
Local storage		Organization unit:	VIV0 ⁻	TEK Inc.		
		Common name:	www.	vivotek.com		
[Basic mode]					Remove certifi	cate
Version: 0100c						

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.

	s				
🗹 Er	Enable HTTPS secure connection				
∞ Mi	✓ Mode: ● HTTP & HTTPS O HTTPS only				
- Ci	ertificate:				
	Certificate information				
	Status:	Active			
	Method:	Create certificate request and i	nstall		
	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		

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	23	Security Information	×
You are about to view Any information you an viewood by anyone oliv In the future, do no	change with first site cannot be a on the Web. It show this warring OK glore Info	This page contains both secure and terms Do you want to display the nonsecure Yes No	nonaecure re ilenis? Mare Inito
Security	Alert		
	 nformation you exchange with this changed by others. However, then security certificate. The security certificate was is not chosen to trust. View the you want to trust the certifyin The security certificate date i The name on the security certificate date i The name on the security certificate date i The name on the security certificate date is 	site cannot be viewed or e is a problem with the site's ssued by a company you have certificate to determine whether g authority. is valid. trificate is invalid or does not	

Security > Access List

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

General Settings

Γ	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 to stream 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 QuickTime Player).

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

IP ac	ldress	Elapsed time	User ID
172.	16.2.53	00:00:05	
192.1	68.4.104	01:49:35	
Refresh	Add to deny list	Disconnect	Close

Note that only consoles that are currently displaying live streaming will be listed in the View Information list.

- 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 that 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 100.
- 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 88.
- 3. The administrator has set up a root password, but allows anonymous viewing. For more information about **Allow Anonymous Viewing**, please refer to page 100.

- 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 Explore or Quick Time Player).

Filter

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

<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. 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.

Film	
EFERN COLESS BOTTONY	
FRAME O ANY & DAY	
en4 access list.	
processing processions	
Add Delete	
\$14 BCC105 BSC	
Front Developments	
Add Dente	

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 > General settings on page 81 for detailed information.

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	- Filter address		
Rule: Single			
IP address: 192.168.2.1			
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 address and network mask are written in CIDR format. For example:

Filter address	
Rule: Network	
Network address / Network mask: 192.168.2.0	/ 24
OK Cancel	

IP address range 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.

vdd ipv6 filter list	
Filter address	
Rule: Network	
Network address / Network mask:	1

<u>Range</u>: This rule allows the user to assign a range of IP addresses to the Allow/Deny List. Note: This rule only applies to IPv4 addresses. 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.

		Save	
	Always allow the IP address to access this device		
	Administrator IP address		
_	A desirietestes ID a data as		

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., your network administrator) which can be validated by a RADIUS server.
- 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).

EEE 802.1x	
Enable IEEE 802.1x	
EAP method:	EAP-PEAP 💌
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.



Security > Miscellaneous

The embedded TrendMicro utitlity provides the protection against Cross-Site Request Forgery. Cross-site request forgery is also known as one-click attack or session riding and is abbreviated as CSRF. CSRF is a type of malicious exploit of a website, in this case, the camera. Unauthorized commands are transmitted from a user that the web application trusts, using the mechanism of forging a trusted user's own request with a request containing his own cookies, etc. Different ways can be used for a malicious website to transmit such commands. They can be specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests. The malicious attack can occur without users' interaction or even knowing it.

-	Miscellaneous
	Enable Cross-Site Request Forgery(CSRF) protection.
	We strongly recommend not to disable this protection. Disabling this feature will expose your camera to risks.
	Save

PTZ > PTZ settings

This section explains how to control the Network Camera's Pan/Tilt/Zoom operation.

Digital: Control the e-PTZ operation. Within a field of view, it allows users to quickly move the focus to a target area for close-up viewing without physically moving the camera.

Digital PTZ Operation (E-PTZ Operation)

The e-PTZ control settings section will be displayed as shown below:

67393	2020/05/20	09:57:30	E	
v1 8			Home	
X1.0	-	-		
-		100	Zoom	111+
		Pan spe	ea.	0
240		Tit spea	id:	0 .
14 P 101	States.	Zoom si	peed:	0
-		Auto par	vpetrol speed:	1 .
Pal	1 and	Go te:	1.000	122
Form location settings Satcurrent pastion as herei Present and patrol settings		Reatore home position to	estant	
Form location settings Satcurrent position as items Preset and patrol settings laris: Add preset location		Restriction to position to a	etaut r Patrol Dw	ell Unic
Formal location settings Satcurrent pasticities home Present and patrol settings farme: [Add present location]] User present locations]] towart loft		Restrictions position to Select Preset Locations fo	setauit r Patrol D e r	ell lime (sec)
Fore location settings Satcurrent paston as hored Present and patrol settings fame: Add preset location User preset locations User preset locations	*	Restrictions position to Select Preset Locations fo Patrol locations upper let	r Patrol De 5	ell lins (sec)
Formal location surflings Satcurrent past ton as home Present and patrol settings fame: [Add/preset locations] [2] User preset locations [2] tower left [2] center [2] road		Restriction to position to a Select Preset Locations fo Patrol locations upper let	r Patrol 5 5	ell lime (sec
Formal location settings Satcurrent pasticities as hores Present and patrol settings famile: [Add present locations] [2] User present locations [2] Iower fail [2] center [2] right [2] useer right	. 8	Restrictions position to a Select Preset Locations fo Patrol locations upper left lower left	etaurt r Patrol 6 5 6	ell lime (sec)
Fore location settings Satcurrent paston as hans Preset and patrol settings latter [Add preset location] [2] User preset locations [2] lower left [2] caller [2] right [2] upper right [2] lower sold		Restrictions position to Select Preset Locations fo Patrol locations upper let lett lower lett center	etauit r Patrol 5 5 5 5 5	ell lime (sec)
Formal location surflings Satcurrent past took as interest Present and patrol settings famile: Add present locations (2) User present locations (2) Iower famil (2) conter (2) right (2) upper right (2) Iower right (2) Iower right (2) Iower right		Restrictions position to Select Preset Locations fo Patrol locations upper let left lower left center inght	r Patrol De 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	ell lime (sec
Formal location surflings Satcurrent pass ton as home Present and patrol settings fame: Add preset locations User preset locations User preset locations User preset locations User preset locations User preset locations User refet User right User right Remove	More	Restrictions position to a Select Preset Locations for Patrol locations upper left left lower left center right Remove	etaurt r Patrol 6 5 6 5 6 6	ell lime (sec
Fore location settings Satcurrent pastoch as hares Preset and patrol settings latte: Add preset location 2 User preset locations 2 lower laft 2 oper laft 2 lower laft 2 upper right 2 lower sett	More	Restrictions position to Select Preset Locations for Patrol locations usper let lett lower lett center right Remove	ertaurt r Patrol 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	ell lime (sec) ii More

For e-PTZ related details, please refer to page 117.

Auto pan/patrol speed: Select the speed from 1~5 (slow/fast) to set up the Auto pan/patrol speed control.

Zoom factor display

If you check this item, the zoom indicator will be displayed on the home page when you zoom in/out the live viewing window as the picture shown on the next page.

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

Home page in the E-PTZ Mode



- The e-Preset Positions will also be displayed on the home page. Select one from the drop-down list, and the Network Camera will move to the selected position.
- If you have set up different preset positions for different streams, you can select one of the video streams to display its separate preset positions.

Global View

In addition to using the e-PTZ control panel, you can also use the mouse to drag or resize the floating frame to pan/tilt/zoom the viewing region. The live view window will also move to the viewing region accordingly.

Moving Instantly

If you check this item, the live view window will switch to the new viewing region instantly after you move the floating frame. If not selected, the process of moving from one position to another will be shown.

Click on Image

The e-PTZ function also supports "Click on Image". When you click on any point of the Global View Window or Live View Window, the viewing region will also move to that point.

Note that the "Click on Image" function only applies when you have configured a smaller "Region of Interest" out of the maximum output frame! e.g., an 800 x 600 region from out of the camera's maximum frame size.

<u>Patrol button</u>: Click this button, then the Network Camera will patrol among the selected preset positions continuously.

Patrol settings

You can select some preset positions for the Network Camera to patrol.

- Please follow the steps below to set up a patrol schedule:
- 1. Select the preset locations on the list, and click \ge .
- 2. The selected preset locations will be displayed on the **Patrol locations** list.
- 3. Set the **Dwelling time** for the preset location during an auto patrol.
- 4. If you want to delete a preset location from the Patrol locations list, select it and click **Remove**.
- 5. Select a location and click **I** to rearrange the patrol order.
- 6. Select patrol locations you want to save in the list and click **Save** to enable the patrol settings.
- 7. To implement the patrol schedule, please go to homepage and click on the **Patrol** button.

CP-V)	2018/3/20	09:57:30	(A)	10
×4 0	-	4	Home	
X1.0	-	-	•	
		-	Zoom	τ.
		Pans	beeq.	0 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Tittsp	eed:	α .
	No.	Zoom	speed:	0 1
· · ·	-	Auto p	pan/patrol speed:	1 1
No - A	100	Gio for	lectone -	-
Home location settings Set current position as home Preset and patrol settings —		Restore home positio	m to default)
Home location settings Set current position as home Preset and patrol settings Came Add preset location		Restore home position	m to default or Patrol	well time
Home location settings Set current position as home Preset and patrol settings — Came Add preset locations User preset locations		Restore home position	n to default or Patrol	wei time (sec)
Home location settings Set current position as home Preset and patrol settings — came Add preset locations User preset locations Upper left I left	^	Restore home positio 2 Select Preset Locations fo Patrol locations Upper left I left	n to default or Patrol	bael time (sec)
Home location settings Set current position as home Preset and patrol settings Kame Add preset location User preset locations User preset locations User preset locations User inft Inft Inft Inft Inft Inft Inft Inft I	^ >	Restore home position	n to default or Patrol	beel time (sec)
Home location settings Set current position as home Preset and patrol settings — Carrie Add preset locations User preset locations User preset locations Upper left Invertieft Conter	*	Restore home position 2 Select Preset Locations for patrol locations Upper left I lower left C center	n to default or Patrol	twell time (sec)
Home location settings Set current position as home Preset and patrol settings Kame Add preset locations User preset locations	*	Restore home position 2 Select Preset Locations fo Patrol locations Upper left I lot I lot I center C center I dobt	or Patrol	beel time (sec)
Home location settings Set current position as home Preset and patrol settings came Add preset locations User preset locations	×	Restore home position 2 Select Preset Locations for Patrol locations Upper left I left I lower Left Conter I right Remove	n to default or Patrol	beel time (sec)
Home location settings Set current position as home Preset and patrol settings — Carne Add preset locations User preset locations User preset locations Upper laft User left Conter Conter Ramous	A P	Restore home position	n to default or Patrol	Aveil time (sec)



- The Preset Positions will also be displayed on the Home page. Select one from the Go to menu, and the Network Camera will move to the selected preset position.
- Click Patrol: The Network Camera will patrol along the selected positions repeatedly.

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. You can configure the Network Camera to send snapshots or videos to your email address or FTP site.

8
9
I
I
I

Event

To configure an event with reactive measures such as recording video or snapshots, it is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. An event is an action initiated by a user-defined trigger source. In the **Event** column, click **Add** to open the event settings window. Here you can arrange three elements -- Schedule, Trigger, and Action to set an event. A total of 3 event settings can be configured.

Event —							
Name	Status Sun	Mon Tue V	Ved Thu	Fri Sa	at Time	Trigger	
Add	Help						
Event name:							
Drable test event							
Prioritic Normal -							- 1
Detect and relation dete	dies te sigitel inp	at other 10	owoond(ii)				
	Erent Sc	tre dute					- I
1 Courses	(if) 194 S	NAN 12 TAN 12	5 mad (2) 11	NEME	i sa		- 1
1. SCHOOL	Time						- 1
		Abays					- 1
_	0	FIRTS III III	f# 24111	\$hnet			- 1
2. Teigger							- 1
							- 1
-							- 1
3.Actus							- 1
							- 1
					0		

- 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 motion detection or digital input after is seconds: Enter the duration in seconds to pause motion detection after a motion is detected. This can prevent event-related actions to take place too frequently.

1. Schedule

Specify the period of time during which the event trigger will take effect. Please select the days of the week and the time in a day (in 24-hr time format) for the event triggering schedule. For example, you may prefer an event to be triggered only during the off-office hours.

2. Trigger

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

There are several choices of trigger sources as shown on the next page. Select the item to display the detailed configuration 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 133 for details.

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

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 and re-connected.

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.

Camera tampering 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 137 for detailed information.

Camera tampering detection

✓ Tampering detection ☐ Too dark ☐ Too bright ☐ Too blurry

Note: Please configure Camera tampering detection first

Manual Triggers

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



1 2 3



VADP

It is presumed that you already uploaded and enabled the VADP modules before you can associatee VADP triggers with an Event setting.

Click on the Set VADP Trigger button to open the VADP setup menu. The triggering conditions available with 3rd-party software modules known as VADP will be listed. Use the arrow buttons to select these triggers. Users may implant these modules for different purposes such as triggering motion detection, or applications related to video analysis, etc. Please refer to page 140 for the configuration options with VADP modules.

Creek Insted		
ADP Triggers	Triggers for Ever	nt Settings
NanualTrigger TriggerA TriggerB TriggerD TriggerD	**	1
	Close	Sava

Once the triggers are configured, they will be listed under the VADP option.

✓ TriggerA ✓ TriggerB TriggerC Set VADP Trigger ManualTrigger ✓ TriggerB < TriggerC	TriggerD	
✓ TriggerB ✓ TriggerC eet VADP Trigger ManualTrigger ✓ TriggerB < TriggerC	TriggerA	
TriggerC et VADP Trigger ManualTrigger >> TriggerD TriggerB TriggerC	V TriggerB	
ManualTrigger >>> TriggerD TriggerA TriggerB TriggerC	TriggerC	
ManualTrigger ManualTrigger TriggerA TriggerB TriggerC	Set VADP Trigger	
	ManualTrigger	>> TriggerD TriggerA TriggerB TriggerC

3. Action

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

Action		
Backup	media if the networ	k is disconnected
Server	Media	Extra parameter
SD	None 💌	SD test View
HTTP	None 💌	
🔲 nas	None 💌	Create folders by date time and hour automatically <u>View</u>
Add serve	er 🔽 Add med	

Backup media if the network is disconnected

Select this option to backup media file on SD card if the network is disconnected. This function will only be displayed after you set up a network storage (NAS). The media to back up can include snapshot images, video, or system logs depending on your event settings.

Add server

It is necessary to configure the server and media settings so that the Network Camera will know what action to take (such as which server to send the media files to) when a trigger is activated. Click **Add server** to open the server setting window. You can specify where the notification messages are sent to 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.

erver name: Email	1	
erver type		
e Email		
Sender email address:	Camera@utvotek.cor	n
Recipient email address:	recipient@vivotek.co	m
Server address:	Ms.vivotek.tw	
Username:	user	
Password:	••••••	
Server port	25	
🛅 This server requires a s	ecure connection (BBL)	
C FTP		
C HTTP		
Network storage		

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 the email address of the sender.
- Recipient email address: Enter the email address of the recipient.
- 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), select **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.

a 110 111 111 1 111 10 11 11 10 10 10 10	3 64 410 1011 111 23 Holdsachermore - 1011 10
The established been sentimeteenfully.	By us in weding would

Click Save server to enable the settings.

Note that after you configure the first event server, the new event server will automatically display on the Server list. If you wish to add other server options, click **Add server**.

	Server	Media			Extra parameter
	SD	None 💌	<u>SD test</u>	<u>View</u>	
	Email	None 💌			
A	dd serve	er 💟 Add med	ia 🔽		

Server type - FTP

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

Server Type	
🖱 Email	
E FTP	
Server address:	tp.vivotek.com
Server port:	21
User name:	wolek
Password	*****
FTP folder name:	
Passive mode	
8 HITP	
Network storage	

- 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 files will be placed. If the folder name does not exist, the Network Camera will automatically 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. The firmware default has the Passive mode checkbox selected.

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://107.168.5.121/cgi-lim/stans/anterver.cgi-	
tp transmission successfully.	



Click Save server to enable the settings.

Server type - HTTP

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

Server Type	
🗇 Email	
© FTP	
👳 нттр	
URL	http://192.168.5.10/cgl-bin/upload.cgl
User name:	
Password	
Password:	

- 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 shown below. If successful, you will receive a test.txt file on the HTTP server.



Click Save server to enable the settings.

Network storage:

Select to send the media files to a networked storage when a trigger is activated. Please refer to **NAS** server on page 146 for details. Note that only one NAS server can be configured.

Click **Save server** to enable the settings.

Server	Media	Extra parameter
E SD	None 💌	SD test View
Email	-None-	2
FTP	-None	1
HTTP [-None-	
I NAS	None	Create folders by date time and hour automatically <u>View</u>

- SD Test: Click to test your SD card. The system will display a message indicating the result as a success or a failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 128 for detailed information.
- View: Click this button to open a file list window. This function is only for SD card and Network Storage. If you click the View button for an SD card, a Local storage page will prompt so that you can manage the recorded files on SD card. For more information about Local storage, please refer to page 148. If you click the View button for a Network storage, a file directory window will prompt for you to view recorded data on Network storage. For detailed illustration, please refer to the next page.
- Create folders by date, time, and hour automatically: If you select this item, the system will automatically create folders by the date when video footages are stored onto the networked storage.

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



Click to delete selected items

Click **20200120** to open the directory:

The format is: HH (24r)

Click to open the file list for that hour

	_														
< (07	<u>08</u>	<u>09</u>	<u>10</u>	<u>11</u>	<u>12</u>	<u>13</u>	<u>14</u> 1	<u>5</u> 1	<u>6</u>	<u>17</u>	≥]		
file name siz							size	3		da	te			time	è
Recording1 58.mp4					mp4	2	5260	004	2020/01/20			07	58	28	
Recording1 59.mp4					mp4	2	5635	536	202	0/0)1/2	20	07	59	28
Delete all Back															
Click to delete selected items								Click t level o	o go f the	bao dir	ck to ecto	o the ory	e prev	ious	6
Click to delete all recorded data															
< (07	<u>08</u>	<u>09</u>	<u>10</u>	<u>11</u>	<u>12</u>	<u>13</u>	<u>14</u> 1	5 1	<u>6</u>	<u>17</u>	≥			

_										
	file name		size	date	time					
	Recording1 58	3.mp4	2526004	2020/01/20	07:58:28					
	Recording1 59).mp4	2563536	2020/01/20	07:59:28					
	Delete Delete all Back									

The format is: File name prefix + Minute (mm)

You can set up the file name prefix on Add media page. Please refer to next page 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:
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
Save media Close

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 any of the video streams.
- Send □ pre-event images

The Network Camera has a buffer to temporarily hold 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 can be generated after a trigger is activated.



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:

Snapshot_20	0200513_100341
1	↑
File name prefix	Date and time suffix The format is: YYYYMMDD_HHMMSS

Click Save media to enable the settings.

Note that 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**.

Media type - Video clip

Select to send video clips when a trigger is activated.

Media Type	
Atlached media:	
Snapshot	
🐵 Video Clip	
Bource: Stream 1 💌	
Pre-event recording: 0 seconds (0-9)	
Maximum duration: 5 seconds [1~20]	
Maximum file size 500 Kbytes (50~4096)	
File name prefix Video Clip_	
System log	
1110.00 - 100.000 - 100.000 - 100.000 - 100.000	

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

The Network Camera has a buffer to temporarily hold data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

Maximum duration

Specify the maximum recording duration in seconds. The duration can be up to 10 seconds. For example, if pre-event recording is set to five seconds and the maximum duration is set to ten 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. Some users may need to stitch the video clips together when searching and packing up forensic evidence.

File name prefix

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

For example:



Click Save media to enable the settings.

Media type - System log

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

Media Type		
Attached media:		
Snapshot		
🙁 Video Citp		
System log		

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

Action Backup r	nedia if the networ	k is disco	nnected		
Server	Media			Extra parameter	
SD	None 💌	<u>SD test</u>	<u>View</u>		
mail <u>Add serve</u>	None None email log snapshot	lia 💟			
				Save event	Close

In the Event settings column, the Servers and Medias you configured will be listed; please make sure the Event -> Status is indicated as **ON**, in order to enable the event triggering action.

When completed, click the **Save event** button to enable the settings and click **Close** to exit Event Settings page. The new Event / Server settings / Media will appear in the event drop-down list on the Event setting page.

Event Status Sun Mon Tue Wed Thu Fri Trigger Name Sat Time 00:00~24:00 ON V V seq event1 V V V Delete Add Help Server settings Address/Location Name Туре HTTP http http://192.168.5.10 Delete Add Media Available memory space: 13000KB Name Туре Snapshot snapshot Delete videoclip Video clip Delete System log systemlog Delete Add Customized script Name Date Time Add

Please see the example of the Event setting page below:

When the Event Status is <u>ON</u>, the event configuration above 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 on the <u>ON</u> button to turn it to <u>OFF</u> status or click the **Delete** button to remove the event setting.

To remove a server setting from the list, select a server name from the drop-down list and click **Delete**. Note that you can only delete a server setting when it is not applied in an existing event setting.

To remove a media setting from the list, select a media name from the drop-down list and click **Delete**. Note that you can only delete a media setting when it is not applied in an existing event setting.

Customized Script

This function allows you to upload a sample script (.xml file) to the camera, 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 technical support.



Applications > Motion detection

This section explains how to configure the Network Camera to enable motion detection. A total of 5 motion detection windows can be configured.



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 4 mouse clicks to designate a detection window. You can change the window shape by dragging the corner marks to a preferred location.
 - Drag the item size tab to change the minimum size of item to trigger an alarm. An item size box will appear in the center of screen for your reference (in semi-transparent red). An intruding object must be larger than the Item size to trigger an alarm. Change the item size according to the live view.
 - To delete a window, click the X mark on the right of the window name.
- 3. Define the sensitivity to moving objects by moving the Sensitivity slide bar. Note that a high sensitivity is prone to produce false alarms such as the fast changes of light (such as day/night mode switch, turning lights on/off). A movement must persist longer than 0.3 second for the motion to be detected.
- 4. Click **Save** to enable the settings.
- 5. Select **Enable motion detection** to enable this function.

12 Graph is due to be the total

For example:

068	Volazione usori il Bio na 7
unite 175	

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 exceed the preset 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 (via an Email or FTP server). For more information on how to configure an event setting, please refer to Event settings on page 119.

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 preset threshold.



If you want to configure other motion detection settings for day/night/schedule mode (e.g., for a different lighting condition), please click **Profile** to open the Motion Detection Profile Settings page as shown below. Another three motion detection windows can be configured on this page.

	000		Window name Motion 1	11
	008	-	AC tem size: 15	
7			Enable to apply	hese settings at
			Night mode	
Sensibility, 80%			Schedule mod	e (nome)

Please follow the steps beolw to set up a profile:

- 1. Create a new motion detection window.
- 2. Click the **Profile mode** tab.
- 3. Select the applicable Schedule mode. Please manually enter a time range.
- 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 select it as a trigger source. Please refer to page 119 for detailed information.



► How does motion detection work?



There are two motion detection parameters: Sensitivity and Min. Item Size. As illustrated above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray in which the sensitivity setting will take effect. Sensitivity is a value that expresses the sensitivity to moving objects. A higher sensitivity setting allows camera to detect slight movements while a lower sensitivity setting will neglect them.

The minimum item size is a threshold value that determines how many "alerted pixels" can trigger an event. When the size of an intruding object is larger than the minimum size, and its movement persist for 0.3 second, the motion is judged to exceed the defined threshold; and the motion window will be outlined in red. With a large minimum item size, the size of moving object in frame C is considered as smaller than the minimum item size, no motion alarm is triggered. With a smaller minimum item size, the same moving object in frame D triggers the alarm.

For applications that require a high level of security management, it is suggested to use **higher** sensitivity settings. However, a higher sensitivity level can also produce false alarms due to fast light changes when switching between the day and night modes, AE switch, turning the light on or off, etc.

Applications > DI and DO

pplications > DI	and DO	
Digital input		
Normal status:	High Cow	
Current status:	High	
Digital output —		
Normal status:	Open Grounded	
	Open	

<u>Digital input</u>: Select High or Low as the Normal status for the digital input connection. 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 126 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 tampering detection	
Tampering detection	
Trigger duration 10 seconds [10~600]	
Trigger threshold 12 [0~100]	
Image too dark detection	
Trigger duration 2 seconds [1~10]	
Trigger threshold 15 [0~100]	
Image too bright detection	
Trigger duration 2 seconds [1~10]	
Trigger threshold 15 [0~100]	
Image too blurry detection	
Trigger duration 7 seconds [1~10]	
Trigger threshold 12 [0~100]	
	Save

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

Click to select the checkbox before tampering conditions: Tampering detection, Image too dark, Image too bright, and Image too blurry. Enter the tamper trigger duration. (10 sec. ~ 10 min.). The duraction specifies the set of time before the tampering is considered as a real alarm. This helps avoid false alarms by short-lived changes.

The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold. Conditions such as image too dark, too bright, or too blurry (defocused) can also be configured as tampering conditions. The Trigger threshold determines how sensitive your is tamper detection setting. Lower the threshold number, easier to trigger.

Too bright: shining a flash light. The average lighting level of the scene is taken into consideration.

Too dark: covering the objective or spraying paint.

Too blurry: blurry scene can be the result of strong interference on the device, such as EMI interference.

2. You can configure Tampering Detection as a trigger element to the proactive event configurations in Event -> Event settings -> Trigger. For example, when the camera is tampered with, camera can be configured to send the pre- and post-event video clips to a networked storage device. Please refer to page 120 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.
- 2. 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		-	
70	n	-	
50	40	∇	
40		5	
30			
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.



- 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.

	30			Alartt Lavel
	80			Valate
	70			
	00			
n e	50			
1	40			
	30			
	20			
	10			
Gene	eral settings nable this profile profile is applied	e to:		
Diss Diss D D N	ey mode light mode			

- 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 80 for Audio settings, and page 70 for video streaming settings.
Applications > Package management - a.k.a., VADP (VIVOTEK Application Development Platform)

Upload package —						
Bave to SD card						
Selectfile				Bro	wee	pload
Resource status						
 Storage status: 						
storage_size:	10240 KBr	tea	Free or	29	10240 KB	rtes
SD card status: De	tached					
Total size:	0 KBytes		Free size:		0 KBytas	
Used size:	0 KBytes		Use (%):		D %6	
Memory status:						
Total size:	24576 KBytes		Free size	ê	24576 KBy	tes
Package list						
Module na	FTNR .	Vander		Version	Status	License
Backso	Debat	Destine	-	Shart		-

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 our 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:

// http://1721662186/cg-bis/admin/upload_vadp.cgi - Windows Internet	Scalar A
: Starting VADP upload procedure, please wait a moment Uploading new module: Hello World / ABC Update configuration . Reloading configuration httpd: . Upload VADP package successfully	
	÷

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

	Module name	Vendor	Version	Status	License	÷
\bigcirc	Hello World	ABC	1.0.0	ON	yes	
	Backup Reload	Restore	Sta	art	Stop	

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.

Package	list					
	Module name	Vendor	Version	Status	License	±
۲	Hello World	ABC	1.0.0	ON	no	
Backu	p Reload	Restore	Sta	art	Stop	

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.

On the License page, register and activate the license for using VIVOTEK's VADP modules. You should acquire the license key elsewhere, and manually upload to the network camera.

Follow the onscreen instruction on VIVOTEK's website for the registration procedure.

Status	License		
— Mai	nual Lic	ense	
To re men	ceive a lice Iber. This (ense key for VADP application, go to device's VADP number is:	http://www.vivotek.com and join the VVTK
BbM	79RE=Od	Gu1PIVEqJRFgc6sacoRs7g4PX(
Sele	ct file	Browse*** No file selected.	Upload

Recording > Recording settings

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

Recording Settings

Recording settings Name Status Sun Mon Tue Wed Thu Fri Sat Time Source Destination Delete Add SD test			 Insert you 	ir SD ca	ard and c	lick he
Name Status Sun Mon Tue Wed Thu Fri Sat Time Source Destination Delete Add SD test SD test	Recording settings					
Add <u>SD test</u>	Name Status Sun M <mark>on T</mark> u	ue Wed Thu Fri	Sat Time	Source	Destination	Delete
	Add <u>SD test</u>					
Note: Before setup recording, you may setup network storage via <u>NAS server</u> page	Note: Before setup recording, ;	you may setup netwo	ork storage via <u>NAS</u>	<u>S server</u> pa	age	



Please remember to format your SD card via the camera's web console (in the Local storage . SD card management page) when using it for the first time. Please refer to page 148 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.

Enable this recording			
With adaptive recording			
Pre-event recording:	5	seconds [0-9]	
Post-event recording:	5	seconds (0-10)	
Priority Normal			
Source: Stream 1 +			
manoontone sommer i	Tri	10ec	
		Schedule	
a. roggar		😨 Sun 😨 Non 😨 Tue 😨 Wed 🗭 Thu 🖉 Fn 😨 Sat	
		Time	
+		· Aways	
2. Destination		From 0200 to 2400 [httmm]	
	0	Network tail	
		0503542444	
Note: To enable recording rid	tricati	on please configure Event first	

- 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, the frame rate will raise up to the value you've configured on the Video quality page. Please refer to page 73 for more information. If you enable adaptive recording on a camera, only when an event is triggered on Camera A will the server record the full frame rate streaming data; otherwise, it will only request the I frame data during normal monitoring, thus effectively saves bandwidths and storage space.



The alarm trigger includes: motion detection and DI detection. Please refer to Event Settings on page 119.

Pre-event recording and post-event recording

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

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



► To enable recording notification please configure *Event settings* first . Please refer to page 119.

Please follow the steps below to set up the recording.

<u>1. Trigger</u>

Select a trigger source.

Conartin		
a schedule		
👿 Sun 👿 Mon 👿 Ti	ie 🗑 Wed 🗑	Thu 🕼 Fn 🔯 Bat
Time		
Alwaya		
D From 00.00	10 24:00	[thinumin]
P. Natwork fail		

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

2. Destination

You can select the SD card or network storage (NAS) for the recorded video files. If you have not configured a NAS server, see details in the following.

	pesanitor
t. Tripper	Destination: nAS
E. Hager	Cepecity.
	E früre free aparts
CONTRACTOR OF	Reserved space: 100 Maytes
2. Destination	Enable cyclic recording
	Recording file management
	Manimum duration (minutes (1-30)
	Maximum file size 100 MB (100-2000)
	File name prefix

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 your server.

For example:

	Add NAS server			
Destination	Server name: NAS	Netv (\\se	vork storage path rver name or IP add	ress\folder na
	Network storage			
	Network storage location;	0192.16	8.5.12WAS	
	(For example; \imy_nasidisk)	(reblot		
	Workgroup:	vivotek		
	User name:	ritial		
	Password			

User name and password for your server

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

http://192.1	68.5.151/cgi-bin/admin/t	estserver 📳 🗖	🔀 http://192.	168.5.151/cgi-bin/	admin/testserver 📰 🗔 🔀
Mount success	fully. Thanks		Mount failed		
Done		Dinternet	Done		🗣 Internet

GO NUMBER	29	- 123
Organism - Sedect acto-m	Brackory Weherpit and Sharing Center View rende printers	
🙀 Facultos	and a second sec	
Decktop	A Date	
Theory Places	Common particular sources	
The artes	Personal August and Au	
Documents		
Pictures		2014 1 42
Veloce	D dest - Notecul	L 10
	File Bolt Format Here the	
2 Canada dan	the second se	
1 controlation	ENDITIETCKICK[The Head is of Sarvier last of Your 19 Cameras	

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

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

Recording name:				
[2] Drazile this recording				
👔 10h adapti-a ra cordinj	(teis)			
Pre-event recording	i 6. excords (0-8)			
Peol-exert recorder	g S seconds(2-10)			
Frienty Normal +				
Neuros: Steam 1 🖝				
	Destination			
1. Trucer	Destination: nag(w)			
	Capacity:			
-	· frite her space			
margin to react the	Esserved Apece 100	Maynee		
2. Destination	Enable cycle recenting			
	Recording file management			
	Bloomen detables: (1 minutes (1-32)			
	Hactment file atom (100 MS (100-500)			
	Fill name partic			
Nate: To examine seconding of	obtables press confours Frent first			
		1	<u> </u>	

- Capacity: You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording. The reserved space is a small amount of space used only for the transaction stage when the capacity is about to be used up or recycled.
- Enable cyclic recording: If you check this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for the transaction stage when the storage space is about to be full and new data arrives. The minimum for the Reserved space must be larger than 15 MegaBytes.
- Recording file management: You can manually assign the Maximum duration and the Maximum file size for each recording footage. You may need to stitch individual files together under some circumstances. You may also designate a file name prefix by filling in the responsive text field.
- File name prefix: Enter the text that will be appended to the front of the file name.

f you want to enable recording notification, please click *Event* to configure event triggering settings. Please refer to **Event > Event settings** on page 119 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. The new recording name will appear in the drop-down list on the recording page as shown below.

To remove a recording setting from the list, select a recording name from the drop-down list and click **Delete**.

Record	ing set	ings										
Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination	Delete
recording	<u>ON</u>	V	۷	V	۷	V	۷	۷	00:00~24:00	stream1	NAS	Delete
Ado	d	<u>s</u>) test									

- Click recording (Name): Opens the Recording Settings page to modify.
- Click ON (Status): The Status will become OFF and stop recording.
- Click <u>NAS</u> (Destination): Opens the file list of recordings as shown below. For more information about folder naming rules, please refer to page 126 for details.

 ⊇0200210 ⊇0200211
⊇ 20200212
Delete Delete all

Storage > SD card management

NOTE:

- It is recommended to turn OFF the recording activity before you remove an SD card from the camera.
- The lifespan of an SD card is limited. Regular replacement of the SD card can be necessary.
- Camera filesystem takes up several megabytes of memory space. The storage space cannot be used for recording.
- Using an SD card that already contains data recorded by another device should not be used in this camera.
- Please do not modify or change the folder names in the SD card. That may result in camera malfunctions.

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: Det	achedn	o SD card						
Total size: 0 KBytesFree size:0 KBytes								
Used size:0 KBytesU	lse (%): 0 %							
			Format					
– SD card status –								
SD card status: Read	ly							
File system: FAT32								
Total size:	15323496 KBytes	Free size:	15087976 KBytes					
Used size:	235520 KBytes	Use (%):	1.537 %					

SD card format

The Linux kernel EXT4 file system format applies to SD card larger than 32GB. However, if EXT4 is applied, the computers running Windows will not be able to access the contents on the SD card unless using some 3rd-party software .

- SD card format		
Ext4		
FAT32	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 the maximum capacity is reached, the oldest file will be overwritten by the latest one.
- 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.

Click **Save** to enable your settings.

NAS management

On the NAS setup page you can configure your NAS (Networked Storage) configuration, test, mount, or unmount the networked storage.

AS setup			
etwork storage lo	cation 11192.168.5.12 DISKSTA	TION	
For example: Vmy	_nas\disktfolder)		
forkgroup:	vivotek		
ser name:	eric.lu		
assword:			
	Text	Mount	Linmount

User name and password for log in to a NAS user account

You can use the **Test** button to check the setting. The result will be shown in the pop-up window.

🗿 http://192.168.5.151	Acgishin Admin/Testserver 🗐 🗖	🔀 🗿 http://192.168.5.151/	🗿 http://192.168.5.151/cgi-bin/admin/testserver 💷 🗇 🔀		
Mount successfully. The	nks	Mount failed			
Done	🜒 Internet	1 Dons	🔮 Internet		

NAS control

NAS control
Minimum reserved storage space: 10 %
Enable cyclic storage
Enable automatic disk cleanup
Maximum duration for keeping files: 7 days
Save

- Minimum reserved storage space: This can be used to configure the percentage of space threshold for the camera commencing space clean-ups. The minimum reserved space is 512MB for SD card; 1GB for a network share.
- Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.
- 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 network share for 7 days.

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** column.

Device target			
All devices	⊖ SD	⊖ nas	
Trigger type			
Backup	System boot	Digital input	
Motion	Network fail	Recording notify	
Periodically	SD card life expectancy	Tampering detection	
VADP	Manual triggers	Audio detection	
Media type			
Video clip	O Snapshot	⊖ Text	
Time			
Search for last	1 minute(s) hours days weeks		
From:	2020/02/26	16 PM	
4	2020/02/04	46	

- File attributes: Select one or more items as your search criteria.
- Trigger time: Manually enter the time range you want to search for contents created at a specific point in time.

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.

Numbers of entries displayed on one page

Searc	n results				
	Name	Trigger type	Starting time	Ending time	
	to SD	Periodically	Today at 3:45 PM	Today at 3:58 PM	Click to open a live vie
	to SD	Periodically	Today at 3:58 PM	-	•
	test	Motion	Today at 3:45 PM	Today at 3:45 PM	
	test	Motion	Today at 3:49 PM	Today at 3:49 PM	
	test	Motion	Today at 3:49 PM	Today at 3:49 PM	
	test	Motion	Today at 3:50 PM	Today at 3:50 PM	
	test	Motion	Today at 3:50 PM	Today at 3:50 PM	
10	~		4	< 1 /3 ► ►	
🛓 Do	wnload 🔒 Lock/	Unlock 🗄 JF	PEGs to AVI	ive	

Play: Click on a search result which will highlight the selected item. A Play window will appear on top for immediate review of the selected file. For example:



- 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 functions 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 checkbox in front of a desired search result, then click this button. The selected items will become Locked, which will not be deleted during cyclic recording. You can click again to unlock the selections. For example:

Searcl	h results				
	Name	Trigger type	Starting time	Ending time	
	to SD	Periodically	Today at 3:45 PM	Today at 3:58 PM	~
	to SD	Periodically	Today at 3:58 PM		
•	test	Motion	Today at 3:45 PM	Today at 3:45 PM	
•	test	Motion	Today at 3:49 PM	Today at 3:49 PM	
✓ ●	test	Motion	Today at 3:49 PM	Today at 3:49 PM	
	test	Motion	Today at 3:50 PM	Today at 3:50 PM	
	test	Motion	Today at 3:50 PM	Today at 3:50 PM	~
10	Y		 		Click to switch pages
🛓 Do	wnload 🔒 Lock/	Jnlock 🗐 JF	PEGs to AVI	ve	

■ 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

2. Style Convention

In URL syntax and in descriptions of CGI parameters, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets shall 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, which is replaced with the string myserver in the URL syntax example, also below.

URL syntax is written with the word "**Syntax:**" written in bold face followed by a box with the reference syntax as seen below. The name of the server is written as <servername>. This 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. Special notes will be marked in RED.

Syntax:

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

Description of returned data is written with "**Return:**" in bold face followed by the returned data shown in a box. All data is returned as HTTP formatted, i.e., starting with the string HTTP and line 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

2. Style Convention

In URL syntax and in descriptions of CGI parameters, a text within angle brackets denotes a content that is to be replaced with either a value or a string. When replacing the text string, the angle brackets shall 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, which is replaced with the string myserver in the URL syntax example, also below.

URL syntax is written with the word "**Syntax:**" written in bold face followed by a box with the reference syntax as seen below. The name of the server is written as <servername>. This 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. Special notes will be marked in RED.

Syntax:

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

Description of returned data is written with "**Return:**" in bold face followed by the returned data shown in a box. All data is returned as HTTP formatted, i.e., starting with the string HTTP and line 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]	viewer	Can view, listen, and talk to camera.
4 [operator]	operator	Operator access rights can modify most of the camera's
		parameters except some privileges and network options.
6 [admin]	admin	Administrator access rights can fully control the
		camera's operations.
7	N/A	Internal APIs. Unable to be changed by any external
		interfaces.

A viewer account can access all APIs with security level 0 and 1. An operator account can access all APIs with security level 0, 1, or 4. An admin account can access all APIs except internal APIs.

Access management is based on the URL directory structure and is described in following paragraphs.

VIVOTEK

5. Get Server Parameter Values

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

Syntax:

Roturn

```
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 oftherelated group will be returned.

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

A successful control request returns parameter pairs as follows:

Actum.
HTTP/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 [<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

Syntax:

http://<servername>/cgi-bin/anonymous/setparam.cgi? <parameter>=<value> [&<parameter>=<value>...][&return=<return page>]

http://<*servername*>/cgi-bin/viewer/setparam.cgi? <*parameter>=<value>* [&<parameter>=<value>...][&return=<return page>]

http://<*servername*>/cgi-bin/operator/setparam.cgi? <*parameter>=<value>* [&<parameter>=<value>...][&return=<return page>]

http://<servername>/cgi-bin/admin/setparam.cgi? <parameter>=<value>
[&<parameter>=<value>...][&return=<return page>]

PARAMETER	DESCRIPTION			
<parameter></parameter>	A full path like: "videoin_c0_s0_h264_resolution",			
	"videoin_c0_s0_h264_maxframe", etc.			
<value></value>	The assigned <value> to the <parameter>.</parameter></value>			
<return page=""></return>	Redirect to the page <return page="">after the <parameter> is assigned. The <return< th=""></return<></parameter></return>			
	page>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). 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.

Example: Set the IP address of server to 192.168.0.123:

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 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></integer>	Any single integer number in 32-bits.		
	The range is -2147483648~2147483647.		
<positive integer=""></positive>	Any single positive integer number in 32-bits.		
	The range is 1~ 4294967295.		
<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=""></ip>	A string limited to an IP address (eg. 192.168.1.1).		
<mac address=""></mac>	A string limited to contain a MAC address without hyphens or colons.		
<boolean></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></text>	SQLite data type. The value is a text string, stored using the database		
	encoding (UTF-8, UTF-16BE or UTF-16-LE).		
<coordinate></coordinate>	x, y coordinate (eg. 0,0)		
<window size=""></window>	window width and height (eg. 800x600)		
<w,h></w,h>	The format for coordinate in 2D.		
	W is the pixel number of width.		
	H is the pixel number of height.		
	EX: (176,144)		

VALID VALUES	DESCRIPTION		
<wxh></wxh>	The format for resolution.		
	W is the pixel number of width.		
	H is the pixel number of height.		
	Ex: 1920x1080, 2048x1536		
available	The API is listed in product WebAPIs.		
non-available	The API is not in product WebAPIs.		
valid	The API is listed in product WebAPIs, and is functional.		
non-valid	The API is listed in product WebAPIs, but is malfunction in this status.		
<decimal></decimal>	Any decimal number expressed in 32-bits ranging from		
	1.18e-38~3.40e+38.		

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

7.1System

Group: system

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
hostname	string[64]	1/6	Host name of server
			(Network Camera,
			Wireless Network Camera,
			Video Server,
			Wireless Video Server).
ledoff	<boolean></boolean>	6/6	Turn on (0) or turn off (1) all led
			indicators.
date	<yyyy dd<="" mm="" td=""><td>6/6</td><td>Current date of system. Set to 'keep' to</td></yyyy>	6/6	Current date of system. Set to 'keep' to
	>,		keep date unchanged. Set to 'auto' to
	keep,		use NTP to synchronize date.
	auto		
time	<hh:mm:ss>,</hh:mm:ss>	6/6	Current time of the system. Set to 'keep'
	keep,		to keep time unchanged. Set to 'auto' to
	auto		use NTP to synchronize time.
datetime	<mmddhhmm< td=""><td>6/6</td><td>Another current time format of the</td></mmddhhmm<>	6/6	Another current time format of the
	YYYY.ss>		system.
ntp	<domain< td=""><td>6/6</td><td>NTP server.</td></domain<>	6/6	NTP server.
	name>,		*Do not use "skip to invoke default
	<ip address="">,</ip>		server" for default value.

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
	<blank></blank>		
timezoneindex	-489 ~ 529	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, London
			40: GMT 01:00 Amsterdam, Berlin,
			Rome, Stockholm, 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 Lebanon, Minsk
			83: GMT 02:00 Israel

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
			120: GMT 03:00 Baghdad, Kuwait,
			Riyadh, Moscow, St. Petersburg, Nairobi
			121: GMT 03:00 Iraq
			140: GMT 03:30 Tehran
			160: GMT 04:00 Abu Dhabi, Muscat,
			Baku,
			Tbilisi, Yerevan
			180: GMT 04:30 Kabul
			200: GMT 05:00 Ekaterinburg, Islamabad,
			Karachi, Tashkent
			220: GMT 05:30 Calcutta, Chennai,
			Mumbai, New Delhi
			230: GMT 05:45 Kathmandu
			240: GMT 06:00 Almaty, Novosibirsk,
			Astana, Dhaka, Sri Jayawardenepura
			260: GMT 06:30 Rangoon
			280: GMT 07:00 Bangkok, Hanoi, Jakarta,
			Krasnoyarsk
			320: GMT 08:00 Beijing, Chongging,
			Hong Kong, Kuala Lumpur, Singapore,
			Taipei
			360: GMT 09:00 Osaka, Sapporo, Tokyo,
			Seoul, Yakutsk
			380: GMT 09:30 Adelaide, 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>	6/6	Enable automaticdaylight saving time in
			time zone.
daylight_dstactualmod	<positive< td=""><td>6/7</td><td>Check if current time is under daylight</td></positive<>	6/7	Check if current time is under daylight
е	integer>		saving time.
			(Used internally)

		100	_	_	
	/ / /				1
- i - i - i - i - i - i - i - i - i - i	r m.,			_	鱼

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
daylight_auto_begintim	string[19]	6/7	Display the current daylight saving start
е			time.
daylight_auto_endtime	string[19]	6/7	Display the current daylight saving end
			time.
daylight_timezones	string	6/6	List time zone index which support
			daylight saving time.
updateinterval	0,	6/6	0 to Disable automatic time adjustment,
	3600,		otherwise, it indicates the seconds
	86400,		between NTP automatic update
	604800,		intervals.
	2592000		
restore	0,	7/6	Restore the system parameters to default
	<positive< td=""><td></td><td>values after <value> seconds.</value></td></positive<>		values after <value> seconds.</value>
	integer>		
reset	0,	7/6	Restart the server after <value> seconds</value>
	<positive< td=""><td></td><td>if <value> is non-negative.</value></td></positive<>		if <value> is non-negative.</value>
	integer>		
restoreexceptnet	0,	7/6	Restore the system parameters to default
	<positive< td=""><td></td><td>values except (ipaddress, subnet, router,</td></positive<>		values except (ipaddress, subnet, router,
	integer>		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	0,	7/6	Restore the system parameters to default
	<positive< td=""><td></td><td>values except all daylight saving time</td></positive<>		values except all daylight saving time
	integer>		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	0,	7/6	Restore the system parameters to default

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
	<positive< td=""><td></td><td>values except the custom language file</td></positive<>		values except the custom language file
	integer>		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	0,	7/6	Restore the system parameters to default
	<positive< td=""><td></td><td>values except the vadp parameters and</td></positive<>		values except the vadp parameters and
	integer>		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.
restoreexceptfocusvalu	0,	7/6	Restore the system parameters to default
е	<positive< td=""><td></td><td>values except zoom and focus value.</td></positive<>		values except zoom and focus value.
	integer>		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.
			* Only available when
			"capability_image_c<0~(n-1)>_remotefo
			cus" != 0.
restoreexceptlen	0,	7/6	Restore the system parameters to default
	<positive< td=""><td></td><td>values except lens profile.</td></positive<>		values except lens profile.
	integer>		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.

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
			* Only available when
			"capability_image_c<0~(n-1)>_lensconfig
			uration_support" != 0.

7.1.1 System.Info

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

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
modelname	string[40]	0/7	Internal model name of the server
extendedmodelname	string[40]	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 address=""></mac>	1/7	12 characters MAC address (without
			hyphens).
firmwareversion	string[40]	0/7	Firmware version, including model,
			company, and version number in the
			format: <model-brand-version></model-brand-version>
language_count	<positive< td=""><td>0/7</td><td>Number of webpage languages available</td></positive<>	0/7	Number of webpage languages available
	integer>		on the server.
language_i<0~(count-	string[16]	0/7	Available language lists.
1)>	language_i0 :		
	English		
	language_i1 :		
	Deutsch		
	language_i2 :		
	Español		
	language_i3 :		
	Français		
	language_i4 :		
	Italiano		
	language_i5 :		
	日本語		
	language_i6 :		
	Português		

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
	language_i7 : 简体中文		
	language_i8 : 繁體中文		
customlanguage_max	0, <positive< td=""><td>0/6</td><td>Maximum number of custom languages</td></positive<>	0/6	Maximum number of custom languages
count	integer>		supported on the server.
customlanguage_coun	0, <positive< td=""><td>0/6</td><td>Number of custom languages which have</td></positive<>	0/6	Number of custom languages which have
t	integer>		been uploaded to the server.
customlanguage_i<0~	string	0/6	Custom language name.
(maxcount-1)>			

7.2Status

Group: status

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
di_i<0~(capability_ndi-1)>	<boolean></boolean>	1/7	0 => Inactive, normal
<product dependent=""></product>			1 => Active, triggered
			(capability_ndi > 0)
do_i<0~(capability_ndo-1)>	<boolean></boolean>	1/7	0 => Inactive, normal
<product dependent=""></product>			1 => Active, triggered
			(capability_ndo > 0)
onlinenum_rtsp	0, <positive< td=""><td>6/7</td><td>Current number of RTSP</td></positive<>	6/7	Current number of RTSP
	integer>		connections.
onlinenum_httppush	0, <positive< td=""><td>6/7</td><td>Current number of HTTP push server</td></positive<>	6/7	Current number of HTTP push server
	integer>		connections.
onlinenum_sip	0, <positive< td=""><td>6/7</td><td>Current number of SIP connections.</td></positive<>	6/7	Current number of SIP connections.
	integer>		
eth_i0	<string></string>	1/7	Get network information from
			mii-tool.
vi_i<0~(capability_nvi-1)>	<boolean></boolean>	1/7	Virtual input
<product dependent=""></product>			0 => Inactive
			1 => Active
			(capability_nvi > 0)

7.2.1 Status per Channel

Group: status_c<0~(n-1)> for n channel products

n denotes the value of "capability_nvideoin"

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
signal_detect	<boolean></boolean>	1/7	Indicates whether the video source is
			connected or not.
			* Only available when
			capability_videoin_type is 0 or 1.
signal_type	ntsc,pal	1/7	The actual modulation type.
			* Only available when
			capability_videoin_type is 0 or 1.

7.3 Digital Input Behavior Define

Group: **di_i<0~(n-1)>** for n is the value of "capability_ndi" (capability_capability_ndi > 0)

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

7.4 Digital Output Behavior Define

Group: do_i<0~(n-1)> for n is the value of "capability_ndo" (capability_ndo > 0)

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

7.5Security

1. Group: security

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
privilege_do	view, operator,	1/6	Indicate which privileges and above
	admin		can control digital output
			(capability_ndo > 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
privilege_camctrl	view, operator,	1/6	Indicate which privileges and above
	admin		can control PTZ
			(capability_ptzenabled > 0 or
			capability_eptz > 0)
user_i0_name	string[64]	6/7	User name of root
user_i<1~20>_name	string[64]	6/7	User name
user_i0_pass	password[64]	7/6	Root password
user_i<1~20>_pass	password[64]	7/6	User password
user_i0_privilege	view,	6/7	Root privilege
	operator,		
	admin		
user_i<1~20>_ privilege	view,	6/6	User privilege
	operator,		
	admin		

7.6Network

Group: network

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
preprocess	<positive integer=""></positive>	6/6	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.

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
			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=5556&
			network_rtp_videoport=20480"
type	lan,	6/6	Network connection type.
	рррое		
resetip	<boolean></boolean>	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>	6/6	IP address of server.
subnet	<ip address=""></ip>	6/6	Subnet mask.
router	<ip address=""></ip>	6/6	Default gateway.
dns1	<ip address=""></ip>	6/6	Primary DNS server.
dns2	<ip address=""></ip>	6/6	Secondary DNS server.
wins1	<ip address=""></ip>	6/6	Primary WINS server.
wins2	<ip address=""></ip>	6/6	Secondary WINS server.

7.6.1 802.1x

Subgroup of network: ieee8021x (capability_protocol_ieee8021x > 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
enable	<boolean></boolean>	6/6	Enable/disable IEEE 802.1x
eapmethod	eap-peap, eap-tls	6/6	Selected EAP method
identity_peap	string[64]	6/6	PEAP identity
identity_tls	string[64]	6/6	TLS identity
password	string[200]	7/6	Password for TLS

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
privatekeypassword	string[200]	7/6	Password for PEAP
ca_exist	<boolean></boolean>	6/6	CA installed flag
ca_time	0, <positive< td=""><td>6/7</td><td>CA installed time. Represented in</td></positive<>	6/7	CA installed time. Represented in
	integer>		EPOCH
ca_size	0, <positive< td=""><td>6/7</td><td>CA file size (in bytes)</td></positive<>	6/7	CA file size (in bytes)
	integer>		
certificate_exist	<boolean></boolean>	6/6	Certificate installed flag (for TLS)
certificate_time	0, <positive< td=""><td>6/7</td><td>Certificate installed time. Represented</td></positive<>	6/7	Certificate installed time. Represented
	integer>		in EPOCH
certificate_size	0, <positive< td=""><td>6/7</td><td>Certificate file size (in bytes)</td></positive<>	6/7	Certificate file size (in bytes)
	integer>		
privatekey_exist	<boolean></boolean>	6/6	Private key installed flag (for TLS)
privatekey_time	0, <positive< td=""><td>6/7</td><td>Private key installed time. Represented</td></positive<>	6/7	Private key installed time. Represented
	integer>		in EPOCH
privatekey_size	0, <positive< td=""><td>6/7</td><td>Private key file size (in bytes)</td></positive<>	6/7	Private key file size (in bytes)
	integer>		

7.6.2 QOS

Subgroup of network: qos_cos (capability_protocol_qos_cos > 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
enable	<boolean></boolean>	6/6	Enable/disable CoS (IEEE 802.1p)
vlanid	1~4095	6/6	VLAN ID
video	0~7	6/6	Video channel for CoS
audio	0~7	6/6	Audio channel for CoS
<product dependent=""></product>			(capability_naudioin > 0)
eventalarm	0~7	6/6	Event/alarm channel for CoS
management	0~7	6/6	Management channel for CoS
eventtunnel	0~7	6/6	Event/Control channel for CoS

Subgroup of network: qos_dscp (capability_protocol_qos_dscp > 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
enable	<boolean></boolean>	6/6	Enable/disable DSCP
video	0~63	6/6	Video channel for DSCP

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
audio	0~63	6/6	Audio channel for DSCP
			(capability_naudioin > 0)
eventalarm	0~63	6/6	Event/alarm channel for DSCP
management	0~63	6/6	Management channel for DSCP
eventtunnel	0~63	6/6	Event/Control channel for DSCP

7.6.3 IPV6

Subgroup of network: ipv6 (capability_protocol_ipv6 > 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
enable	<boolean></boolean>	6/6	Enable IPv6.
addonipaddress	<ip address=""></ip>	6/6	IPv6 IP address.
addonprefixlen	0~128	6/6	IPv6 prefix length.
addonrouter	<ip address=""></ip>	6/6	IPv6 router address.
addondns	<ip address=""></ip>	6/6	IPv6 DNS address.
allowoptional	<boolean></boolean>	6/6	Allow manually setup of IP address
			setting.

7.6.4 FTP

Subgroup of network: ftp

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
port	21, 1025~65535	6/6	Local ftp server port.
enable	<boolean></boolean>	6/6	Enable ftp.
7.6.5 HTTP

Subgroup of network: http

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
port	80, 1025 ~	1/6	HTTP port.
	65535		
alternateport	1025~65535	6/6	Alternate HTTP port.
authmode	basic,	1/6	HTTP authentication mode.
	digest		
s<0~(capability_nmed	string[32]	1/6	Http server push access name for stream
iastream-1)>_accessn			N, N= 1~ capability_nmediastream.
ame			<pre>(capability_protocol_spush_mjpeg =1</pre>
<product dependent=""></product>			and capability_nmediastream > 0)
<not recommended<="" td=""><td></td><td></td><td>The value are shown as</td></not>			The value are shown as
to use this>			<pre>video1s1.mjpg = c0_s0_accessname,</pre>
			(channel1stream1)
			<pre>video1s2.mjpg = c0_s1_accessname,</pre>
			(channel1stream2)
			<pre>video1s3.mjpg = c0_s2_accessname,</pre>
			(channel1stream3)
			<pre>video1s4.mjpg = c0_s3_accessname,</pre>
			(channel1stream4)
			etc.
			* We replace this parameter with
			"network_http_c<0~(capability_nvideoin
			-1)>_s<0~(capability_nmediastream-1)>_
			accessname
			" when the version number (httpversion)
			is equal or greater than 0311c.
anonymousviewing	<boolean></boolean>	1/6	Enable anonymous streaming viewing.

7.6.6 HTTP per Channel

Subgroup of **network**: http_c<0~(n-1)> for n channel products

n denotes the value of "capability_nvideoin"

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
s<0~(capability_nmedia	string[32]	1/6	Http server push access name for
stream-1)>_accessname			channel N and stream M, N= 1~
<product dependent=""></product>			capability_nvideoin, M= 1~
			capability_nmediastream.
			<pre>(capability_protocol_spush_mjpeg =1</pre>
			and capability_nmediastream > 0)
			The value are shown as
			<pre>video1s1.mjpg = c0_s0_accessname,</pre>
			(channel1stream1)
			<pre>video1s2.mjpg = c0_s1_accessname,</pre>
			(channel1stream2)
			<pre>video2s1.mjpg = c1_s0_accessname,</pre>
			(channel2stream1)
			<pre>video2s2.mjpg = c1_s1_accessname,</pre>
			(channel2stream2)
			etc.
			* We support this parameter when the
			version number (httpversion) is equal or
			greater than 0311c.

7.6.7 HTTS Port

Subgroup of network: https (capability_protocol_https > 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
port	443, 1025 ~	1/6	HTTPS port.
	65535		

7.6.8 RTSP

Subgroup of network: rtsp (capability_protocol_rtsp > 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
port	554, 1025 ~ 65535	1/6	RTSP port.
			(capability_protocol_rtsp=1)
anonymousviewing	<boolean></boolean>	1/6	Enable anoymous streaming
			viewing.
authmode	disable,	1/6	RTSP authentication mode.
	basic,		(capability_protocol_rtsp=1)
	digest		
s<0~(capability_nmed	string[32]	1/6	RTSP access name for
iastream*capability_n			channel/stream N, N= 1~
videoin)-1)>_accessna			capability_nmediastream.
me			(capability_protocol_spush_mjpeg
<product dependent=""></product>			=1 and capability_nmediastream > 0)
			The value are shown as
			live1s1.sdp = c0_s0_accessname,
			(channel1stream1)
			live1s2.sdp = c0_s1_accessname,
			(channel1stream2)
			live1s3.sdp = c0_s2_accessname,
			(channel1stream3)
			live1s4.sdp = c0_s3_accessname,
			(channel1stream4)
			etc.

7.6.9 RTSP Multicast

Subgroup of network_rtsp_s<0~(n-1)>_multicast

n denotes the value of "capability_nmediastream * capability_nvideoin"

	· /_		· ,=
NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
alwaysmulticast	<boolean></boolean>	4/4	Enable always multicast.
ipaddress	<ip< td=""><td>4/4</td><td>Multicast video IP address.</td></ip<>	4/4	Multicast video IP address.
	address>		* We replace

1/1	V	0		1/
VI	V	υ		\mathbf{A}

NAME	VALUE	SECURITY	DESCRIPTION	
		(get/set)		
			"network_rtsp_s<0~(n-1)>_multicast_ipaddress"	
			with "	
			network_rtsp_s<0~(n-1)>_multicast_videoipadd	
			ress ".	
			* Reserved for compatibility, and suggest don't	
			use this since [httpversion] > 0304a	
videoipaddress	<ip< td=""><td>4/4</td><td>Multicast video IP address.</td></ip<>	4/4	Multicast video IP address.	
	address>		* We support this parameter when the version	
			number (httpversion) is equal or greater than	
			0304a.	
audioipaddress	<ip< td=""><td>4/4</td><td>Multicast audio IP address.</td></ip<>	4/4	Multicast audio IP address.	
<product< td=""><td>address></td><td></td><td>* We support this parameter when the version</td></product<>	address>		* We support this parameter when the version	
dependent>			number (httpversion) is equal or greater than	
			0304a.	
			* Only available when capability_naudioin > 0	
metadataipaddres	<ip< td=""><td>4/4</td><td>Multicast metadata IP address.</td></ip<>	4/4	Multicast metadata IP address.	
S	address>		* We support this parameter when the version	
			number (httpversion) is equal or greater than	
			0304a.	
videoport	1025 ~	4/4	Multicast video port.	
	65535			
audioport	1025 ~	4/4	Multicast audio port.	
<product< td=""><td>65535</td><td></td><td>* Only available when capability_naudioin > 0</td></product<>	65535		* Only available when capability_naudioin > 0	
dependent>				
metadataport	1026~6553	4/4	Multicast metadata port.	
	4			
ttl	1 ~ 255	4/4	Multicasttime to live value.	

7.6.10 SIP Port

Subgroup of network: sip (capability_protocol_sip> 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
port	1025 ~ 65535	1/6	SIP port.

7.6.11 RTP Port

Subgroup of network: rtp

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
videoport	1025 ~ 65535	6/6	Video channel port for RTP.
audioport	1025 ~ 65535	6/6	Audio channel port for RTP.
metadataport	1025 ~ 65535	6/6	Metadata channel port for RTP.

7.6.12 PPPoE

Subgroup of network: pppoe (capability_protocol_pppoe > 0)

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
user	string[128]	6/6	PPPoE account user name.
pass	password[64]	7/6	PPPoE account password.

7.7IP Filter

Group: ipfilter

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
enable	<boolean></boolean>	6/6	Enable access list filtering.
admin_enable	<boolean></boolean>	6/6	Enable administrator IP address.
admin_ip	string[43]	6/6	Administrator IP address.
maxconnection	1~	6/6	Maximum number of (s).
	"capability_protoc		
	ol_maxconnection"		
type	0, 1	6/6	Ipfilter policy :
			0 => allow
			1 => deny
ipv4list_i<0~9>	Single address: <ip< td=""><td>6/6</td><td>IPv4 address list.</td></ip<>	6/6	IPv4 address list.
	address>		
	Network address:		
	<ip <="" address="" td=""><td></td><td></td></ip>		
	network mask>		

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
	Range		
	address: <start ip<="" td=""><td></td><td></td></start>		
	address - end ip		
	address>		
ipv6list_i<0~9>	string[43]	6/6	IPv6 address list.

7.8Video Input

Group: **videoin**

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
cmosfreq	50, 60	4/4	CMOS frequency.
			* Only available when
			capability_videoin_type is 2.
whitebalance	auto,	4/4	Modes of white balance.
<product dependent=""></product>	panorama,		"auto": Auto white balance
	manual,		"panorama": indicates that camera
	rbgain,		would try to balance the white
	widerange,		balance effect of every sensor.
	outdoor,		"rbgain": Use rgain and bgain to set
	indoor,		white balance manually.
	sodiumauto,		"manual": 2 cases:
	etc		a. if "rbgain" is not supported, this
			means keep current white balance
	(Available values		status.
	are listed in		b. if "rbgain" is supported, "rgain"
	"capability_image_		and "bgain" are updated to the
	c<0~(n-1)>_wbmo		current values which is got from
	de")		white balance module. Then, act as
			rbgain mode
			"widerange": Auto Tracing White
			balance (2000K to 10000K).
			"outdoor": auto white balance mode
			specifically for outdoor.
			"indoor": auto white balance mode
			specifically for indoor.

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
			"sodiumauto": sodium vapor lamps.
			* Only available when
			"capability_image_c<0~(n-1)>_wbmo
			de" !="-"
exposurelevel	0~12	4/4	Exposure level
			"0,12": This range takes the concept
			from DC's exposure tuning options.
			The definition is:
			0: EV -2.0
			1: EV -1.7
			2: EV -1.3
			3: EV -1.0
			4: EV -0.7
			5: EV -0.3
			6: EV 0
			7: EV +0.3
			8: EV +0.7
			9: EV +1.0
			10: EV +1.3
			11: EV +1.7
			12: EV +2.0
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_mode" !=0
irismode	fixed, indoor,	4/4	Control DC-Iris mode.
	outdoor		"outdoor": Auto-setting DC-Iris to get
	<product< td=""><td></td><td>best quality, but easy to meet rolling</td></product<>		best quality, but easy to meet rolling
	independent>		or flicker effect in indoor
			environment.
			"indoor": Avoid rolling and flicker
			effect first.
			"fixed": Open the iris to maximum.
			* Only available when
			capability_image_c<0~(n-1)>_iristype
			"=dciris
enableblc	<boolean></boolean>	4/4	Enable backlight compensation.

VALUE	SECURITY	DESCRIPTION
	(get/set)	
		* Not support this parameter
		anymore when the version number
		(httpversion) is equal or greater than
		0301a.
		* It's recommanded to use
		"exposurewin_c<0~(n-1)>_mode" to
		switch on/off BLC.
0, 1	4/4	0 =>monochrome
		1 => color
		* Only available when "
		capability_videoin_c<0~(n-1)>_color_
		support" is 1.
<boolean></boolean>	4/4	Flip the image.
<boolean></boolean>	4/4	Mirror the image.
0,90,180,270	1/4	The rotation angle of image.
		Support only in Rotation mode.
		* Only available when "
		capability_videoin_c<0~(n-1)>_rotatio
		n"=1
0, <positive< td=""><td>1/7</td><td>A 32-bit integer, each bit can be set</td></positive<>	1/7	A 32-bit integer, each bit can be set
integer>		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;
		O(not support), 1(support)(SD/PZ/IZ
1	1	1
		series only)
-	VALUE VALUE 0, 1 0, 1 <boolean> <boolean> 0,90,180,270 0,<positive integer=""></positive></boolean></boolean>	VALUESECURITY (get/set)0, 14/40, 14/4 <boolean>4/4<boolean>4/40,90,180,2701/40,<positive </positive integer>1/7</boolean></boolean>

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
imprinttimestamp	<boolean></boolean>	4/4	Overlay time stamp on video.
minexposure	<1~32000>,	4/4	Minimum exposure time
<product dependent=""></product>	<5~32000>,		1~32000 => 1s ~ 1/32000s
	<1~8000>,		5~32000 => 1/5s ~ 1/32000s
	<5~8000>,		1~8000 => 1s ~ 1/8000s
	etc.		5~8000 => 1/5s ~ 1/8000s
			etc.
	* Available value is		* Only available when
	listed in		"capability_image_c<0~(n-1)>_exposu
	"capability_image_		re_minrange" != "-"
	c<0~(n-1)>_exposu		* Only valid when
	re_minrange"		"piris_mode"=manual or
			"irismode"=fixed
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_rangetype" is "twovalues".
maxexposure	<1~32000>,	4/4	Maximum exposure time
<product dependent=""></product>	<5~32000>,		1~32000 => 1s ~ 1/32000s
	<1~8000>,		5~32000 => 1/5s ~ 1/32000s
	<5~8000>,		1~8000 => 1s ~ 1/8000s
	etc.		5~8000 => 1/5s ~ 1/8000s
			etc.
	* Available value is		* This parameter may also restrict
	listed in		image frame rate from sensor due to
	"capability_image_		sensor generates a frame per
	c<0~(n-1)>_exposu		exposure time. Ex: If this is set to 1/5s
	re_maxrange"		~ 1/8000s and camera takes 1/5s on
			the night, then sensor only outputs 5
			frame/s.
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_maxrange" != "-"
			* Only valid when
			"piris_mode"=manual or
			"irismode"=fixed
			* Only available when

NAME	VALUE	SECURITY	DESCRIPTION
		(get/set)	
			"capability_image_c<0~(n-1)>_exposu
			re_rangetype" is "twovalues".
enablepreview	<boolean></boolean>	1/4	Usage for UI of exposure settings.
			Preview settings of video profile.
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_mode" !=0

7.8.1 Video Input Setting per Channel

Group: videoin_c<0~(n-1)> for n channel products, and m is stream number n denotes the value of "capability_nvideoin", m denotes the value of "capability_nmediastream"

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
cmosfreq	50, 60	4/4	CMOS frequency.
			* Only available when "
			capability_videoin_type " is 2
mode	0~	4/4	Indicate the video mode on use.
	"capability_videoin_c<0~(
	n-1)>_nmode"-1		
whitebalance	auto,	4/4	Modes of white balance.
<product< td=""><td>panorama,</td><td></td><td>"auto": Auto white balance</td></product<>	panorama,		"auto": Auto white balance
dependent>	manual,		"panorama": indicates that camera
	rbgain,		would try to balance the white
	widerange,		balance effect of every sensor.
	outdoor,		"rbgain": Use rgain and bgain to set
	indoor,		white balance manually.
	sodiumauto,		"manual": 2 cases:
	etc		a. if "rbgain" is not supported, this
			means keep current white balance
	(Available values are listed		status.
	in		b. if "rbgain" is supported, "rgain"
	"capability_image_c<0~(n-		and "bgain" are updated to the
	1)>_wbmode")		current values which is got from
			white balance module. Then, act as
			rbgain mode
			"widerange": Auto Tracing White
			balance (2000K to 10000K).
			"outdoor": auto white balance mode
			specifically for outdoor.
			"indoor": auto white balance mode
			specifically for indoor.
			"sodiumauto": sodium vapor lamps.
			* Only available when
			"capability_image_c<0~(n-1)>_wbmo

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			de" !="-"
rgain	0~100	4/4	Manual set rgain value of gain control
			setting.
			0: Weak <-> 100: Strong
			* Only available when "rbgain" is
			listed in
			"capability_image_c<0~(n-1)>_wbmo
			de".
			* Only valid when
			"videoin_c<0~(n-1)>_whitebalance" !
			= auto
			* Normalized range.
bgain	0~100	4/4	Manual set bgain value of gain control
			setting.
			0: Weak <-> 100: Strong
			* Only available when "rbgain" is
			listed in
			"capability_image_c<0~(n-1)>_wbmo
			de".
			* Only valid when
			"videoin_c<0~(n-1)>_whitebalance" !
			= auto
			* Normalized range.
exposurelevel	0~12	4/4	Exposure level
			"0,12": This range takes the concept
			from DC's exposure tuning options.
			The definition is:
			0: EV -2.0
			1: EV -1.7
			2: EV -1.3
			3: EV -1.0
			4: EV -0.7
			5: EV -0.3
			6: EV 0
			7: EV +0.3
			8: EV +0.7

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			9: EV +1.0
			10: EV +1.3
			11: EV +1.7
			12: EV +2.0
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_mode" !=0
exposuremode	auto,	4/4	Select exposure mode.
<product< td=""><td>shutterpriority,</td><td></td><td>"auto": Automatically adjust the Iris,</td></product<>	shutterpriority,		"auto": Automatically adjust the Iris,
dependent>	irispriority,		Gain and Shutter Speed to fit the
	qualitypriority,		exposure level.
	manual,		"shutterpriority": Manually adjust
	etc		with variable Shutter Speed, and keep
			adjusting Iris, Gain automatically.
	(Available options are list		"irispriority": Manually adjust with
	in		variable Iris, and keep adjusting Gain
	"capability_image_c<0~(n-		and Shutter speed automatically.
	1)>_exposure_modetype")		"qualitypriority": Automatically
			adjust the Iris, Gain and Shutter Speed
			by VIVOTEK quality algorithm.
			"manual": Manually adjust with
			variable Shutter, Iris and Gain.
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0302a.
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_mode" !=0
irismode	fixed, indoor, outdoor	4/4	Control DC-Iris mode.
	<product dependent=""></product>		"outdoor": Auto-setting DC-Iris to get
			best quality, but easy to meet rolling
			or flicker effect in indoor
			environment.
			"indoor": Avoid rolling and flicker
			effect first.
			"fixed": Open the iris to maximum.

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			* Only available when
			"capability_image_c<0~(n-1)>_iristype
			"=dciris
piris_mode	manual, indoor, outdoor,-	1/4	Control P-Iris mode.
<product< td=""><td></td><td></td><td>"outdoor": Auto-setting P-Iris to get</td></product<>			"outdoor": Auto-setting P-Iris to get
dependent>			best quality, but easy to meet rolling
			or flicker effect in indoor
			environment.
			"indoor": Avoid rolling and flicker
			effect first.
			"manual": Manual set P-Iris by
			"piris_position".
			"-": not support. (only available when
			"capability_image_c<0~(n-1)>_sensor
			type" is "smartsensor")
			* Only available when
			"capability_image_c<0~(n-1)>_iristype
			"=piris
piris_position	1~100	1/4	Manual set P-Iris.
<product< td=""><td></td><td></td><td>1: Open <-> 100: Close</td></product<>			1: Open <-> 100: Close
dependent>			* Only valid when
			"piris_mode"=manual or
			"capability_image_c<0~(n-1)>_sensor
			type" is "smartsensor"
			* Only available when
			"capability_image_c<0~(n-1)>_iristype
			"=piris
enableblc	<boolean></boolean>	4/4	Enable backlight compensation
<not support<="" td=""><td></td><td></td><td>* Not support this parameter</td></not>			* Not support this parameter
anymore>			anymore when the version number
			(httpversion) is equal or greater than
			0301a.
			* It's recommanded to use
			"exposurewin_c<0~(n-1)>_mode" to
			switch on/off BLC.
maxgain	0~100	4/4	Maximum gain value.

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			0: Low <-> 100: High
			* Only available when
			"capability_image_c<0~(n-1)>_agc_m
			axgain" != "-"
			* Only valid when
			"piris_mode"=manual or
			"irismode"=fixed
			* Normalized range.
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_rangetype" is "twovalues".
mingain	0~100	4/4	Minimum gain value.
			0: Low <-> 100: High
			* Only available when
			"capability_image_c<0~(n-1)>_agc_mi
			ngain" != "-"
			* Only valid when
			"piris_mode"=manual or
			"irismode"=fixed
			* Normalized range.
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_rangetype" is "twovalues".
gainvalue	0~100	4/4	Gain value.
			0: Low <-> 100: High
			* Only available when
			"capability_image_c<0~(n-1)>_agc_m
			axgain" != "-" and
			"capability_image_c<0~(n-1)>_exposu
			re_rangetype" is "onevalue".
			* Normalized range.
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0302a.
color	0, 1	4/4	0 =>monochrome
			1 => color

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			* Only available when "
			capability_videoin_c<0~(n-1)>_color_
			support" is 1.
flip	<boolean></boolean>	4/4	Flip the image.
mirror	<boolean></boolean>	4/4	Mirror the image.
rotate	0,90,180,270	1/4	The rotation angle of image.
			Support only in Rotation mode
			(capability_videoin_c<0~(n-1)>_rotati
			on=1)
ptzstatus	0, <positive integer=""></positive>	1/7	A 32-bit integer, each bit can be set
<not support<="" td=""><td></td><td></td><td>separately as follows:</td></not>			separately as follows:
anymore>			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;
			O(not support), 1(support)
			Bit 5 => Support focus operation;
			O(not support), 1(support)(SD/PZ/IZ
			series only)
text	string[64]	1/4	Enclose caption.
imprinttimesta	<boolean></boolean>	4/4	Overlay time stamp on video.
mp			
textonvideo_p	top, bottom	4/4	Text on video string position
osition			
textonvideo_si	20~40	4/4	Text on video font size
ze			
textonvideo_fo	/usr/share/font/Default.ttf	4/4	Choose camera default font file
ntpath	, /mnt/flash2/upload.ttf		(/usr/share/font/Default.ttf) or user
			uploaded font
			file(/mnt/flash2/upload.ttf).
textonvideo_u	Depends on the font file	1/7	Show the uploaded font file name.

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
ploadfilename	name uploaded by user		
minexposure	<1~32000>,	4/4	Minimum exposure time
<product< td=""><td><5~32000>,</td><td></td><td>1~32000 => 1s ~ 1/32000s</td></product<>	<5~32000>,		1~32000 => 1s ~ 1/32000s
dependent>	<1~8000>,		5~32000 => 1/5s ~ 1/32000s
	<5~8000>,		1~8000 => 1s ~ 1/8000s
	etc.		5~8000 => 1/5s ~ 1/8000s
			etc.
	* Available value is listed		* Only available when
	in		"capability_image_c<0~(n-1)>_exposu
	"capability_image_c<0~(n-		re_minrange" != "-"
	1)>_exposure_minrange"		* Only valid when
			"piris_mode"=manual or
			"irismode"=fixed
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_rangetype" is "twovalues".
maxexposure	<1~32000>,	4/4	Maximum exposure time
<product< td=""><td><5~32000>,</td><td></td><td>1~32000 => 1s ~ 1/32000s</td></product<>	<5~32000>,		1~32000 => 1s ~ 1/32000s
dependent>	<1~8000>,		5~32000 => 1/5s ~ 1/32000s
	<5~8000>,		1~8000 => 1s ~ 1/8000s
	etc.		5~8000 => 1/5s ~ 1/8000s
	* Available value is listed		etc.
	in		* This parameter may also restrict
	"capability_image_c<0~(n-		image frame rate from sensor due to
	1)>_exposure_maxrange"		sensor generates a frame per
			exposure time. Ex: If this is set to 1/5s
			~ 1/8000s and camera takes 1/5s on
			the night, then sensor only outputs 5
			frame/s.
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_maxrange" != "-"
			* Only valid when
			"piris_mode"=manual or
			"irismode"=fixed
			* Only available when

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			"capability_image_c<0~(n-1)>_exposu
			re_rangetype" is "twovalues".
shuttervalue	<1~32000>,	4/4	Exposure time
<product< td=""><td><5~32000>,</td><td></td><td>1~32000 => 1s ~ 1/32000s</td></product<>	<5~32000>,		1~32000 => 1s ~ 1/32000s
dependent>	<1~8000>,		5~32000 => 1/5s ~ 1/32000s
	<5~8000>,		1~8000 => 1s ~ 1/8000s
	etc.		5~8000 => 1/5s ~ 1/8000s
			etc.
	* Available value is listed		* This parameter may also restrict
	in		image frame rate from sensor due to
	"capability_image_c<0~(n-		sensor generates a frame per
	1)>_exposure_maxrange"		exposure time. Ex: If this is set to 1/5s
			~ 1/8000s and camera takes 1/5s on
			the night, then sensor only outputs 5
			frame/s.
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_maxrange" != "-" and
			"capability_image_c<0~(n-1)>_exposu
			re_rangetype" is "onevalue".
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0302a.
enablepreview	<boolean></boolean>	1/4	Usage for UI of exposure settings.
			Preview settings of video profile.
			* Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_mode" !=0
meteringmode	auto,	4/4	" auto ": The algorithm chooses the
	blc,		best metering strategy.
	hlc		" blc ": This metering method increases
	* Available value is listed		the weight of dark area.
	in		"hlc": The metering method can
	"capability_image_c<0~(n-		detect strong light and make affected
	1)>_exposure_meteringm		area clear.
	ode"		

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0311a.
crop_position	<coordinate></coordinate>	1/7	Crop left-top corner coordinate.
	(x,y)		
crop_size	<window size=""></window>	1/7	Crop width and height.
	(WxH)		(width must be 16x or 32x and height
			must be 8x)
zoomratiodispl	<boolean></boolean>	1/4	Indicates multiple of zoom in is
ау			"on-screen display" or not.
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0302a.
bracketing_lev	1~100	4/4	 The total available lists
el			(capability_image_c<0~(n-1)>_ex
			posure_bracketing_range) will be
			normalized to 1~100 scale.
			• For example, the total available
			list is 7. (2x,3x,4x,5x,6x,7x,8x)
			• 1 ~ 14 that correspond with 2x.
			• 15 ~ 30 that correspond with 3x.
			*Only available when
			"capability_image_c<0~(n-1)>_exposu
			re_bracketing_mode"=1.
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0310a.
s<0~(m-1)>_en	<boolean></boolean>	4/4	Indicate whether stream supprts eptz
ableeptz			or not
s<0~(m-1)>_co	Listed at	1/4	Codec type for this stream
dectype	"capability_videoin_codec		
	п		
	Possible values are: mjpeg,		
	h264,h265		
	<product dependent=""></product>		
s<0~(m-1)> re	Available options are list in	1/4	Video resolution in pixels.

get/set)		DESCRIPTION	52001111	VALUE	
			get/set)		
solution "capability_videoin_c<0~("capability_videoin_c<0~(solution
n-1)>_resolution".				n-1)>_resolution".	
Besides, available options				Besides, available options	
is referred to				is referred to	
"capability_videoin_c<0~("capability_videoin_c<0~(
n-1)>_maxresolution" and				n-1)>_maxresolution" and	
"capability_videoin_c<0~("capability_videoin_c<0~(
n-1)>_minresolution"				n-1)>_minresolution"	
s<0~(m-1)>_s <boolean> 4/4 Enable "Smart fps" function.</boolean>		Enable "Smart fps" function.	4/4	<boolean></boolean>	s<0~(m-1)>_s
martfps_enabl * Only available when		* Only available when			martfps_enabl
e "capability_videoin_c<0~(n-1)>_smai)>_smai	"capability_videoin_c<0~(n-1)>_s			е
fps_support" is 1.		fps_support" is 1.			
* We support this parameter when	when	* We support this parameter who			
the version number (httpversion) is	ion) is	the version number (httpversion)			
equal or greater than 0309a.		equal or greater than 0309a.			
s<0~(m-1)>_h2 <boolean> 4/4 Enable "Dynamic intra frame period"</boolean>	period"	Enable "Dynamic intra frame per	4/4	<boolean></boolean>	s<0~(m-1)>_h2
64_dintraperio * Only available when		* Only available when			64_dintraperio
d_enable "capability_videoin_c<0~(n-1)>_dintr)>_dintr	capability_videoin_c<0~(n-1)>_			d_enable
period_support" is 1.		period_support" is 1.			
* We support this parameter when	when	* We support this parameter whe			
the version number (httpversion) is	ion) is	the version number (httpversion)			
equal or greater than 0301c.		equal or greater than 0301c.		250 500 4000 2000	
$s<0^{(m-1)}_h2$ 250, 500, 1000, 2000, 4/4 The time interval between two	0	The time interval between two	4/4	250, 500, 1000, 2000,	s<0~(m-1)>_h2
64_Intraperiod 3000, 4000 I-frames (Intra coded picture).		I-frames (Intra coded picture).		3000, 4000	64_intraperiod
The unit is millisecond (ms).		The unit is millisecond (ms).			
s<0~(m-1)>_h2 cbr, vbr 4/4 cbr: Constant bit rate mode.		cbr : Constant bit rate mode.	4/4	cor, vor	s<0~(m-1)>_h2
64_ratecontrol Vbr : Fixed quality mode, all frames ar	ames ar	vbr : Fixed quality mode, all frame			64_ratecontrol
mode encoded in the same quality.	-1	encoded in the same quality.		4.5	mode
s<0°(m-1)>_n2 1°5, 4/4 Set the pre-defined quality level:	vei:	Set the pre-defined quality level:	4/4	1~5,	s<0°(m-1)>_n2
64_quant 99, 100 1: Medium		1: Medium		99, 100	64_quant
2: Standard		2: Standard			
3: G000		5. UUUU			
4: Detailed		4. Delalleu 5. Excollont			
5. Excellent		100: Use the quality lovel in			

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			"qpercent"
			99: Use the quality level in "qvalue"
			* Only valid when
			"h264_ratecontrolmode"= vbr.
s<0~(m-1)>_h2	0~51	4/4	Manual video quality level input. The
64_qvalue			Q value which is used by encoded
			library directly.
			* Only valid when
			"h264_ratecontrolmode"= vbr and
			s<0~(m-1)>_h264_quant = 99.
s<0~(m-1)>_h2	1~100	4/4	Select customized quality in a
64_qpercent			normalized full range.
			1: Worst quality
			100: Best quality
			* Only valid when
			"h264_ratecontrolmode"= vbr and
			"quant"= 100.
s<0~(m-1)>_h2	20000~"capability_videoin	4/4	The maximum allowed bit rate in fixed
64_maxvbrbitr	_c<0~(n-1)>_h264_maxbit		quality mode.
ate	rate"		When the bit rate exceeds this value,
			frames will be dropped to restrict the
			bit rate.
			* Only valid when
			"h264_ratecontrolmode"= vbr
s<0~(m-1)>_h2	1~5, 100	4/4	Set the pre-defined quality level:
64_cbr_quant			1: Medium
			2: Standard
			3: Good
			4: Detailed
			5: Excellent
			100: Use the quality level in
			"cbr_qpercent"
			* Only available when
			"h264_ratecontrolmode"= cbr.
			* Only available when
			"capability smartstream version" >=

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			"2.0"
s<0~(m-1)>_h2	1~100	4/4	Select customized quality in a
64_cbr_qperce			normalized full range.
nt			1: Worst quality
			100: Best quality
			* Only valid when
			"h264_ratecontrolmode"= cbr and
			"quant"= 100.
			* Only available when
			"capability_smartstream_version">=
			"2.0"
s<0~(m-1)>_h2	20000~"capability_videoin	4/4	The target bit rate in constant bit rate
64_bitrate	_c<0~(n-1)>_h264_maxbit		mode.
	rate"		* Only valid when
			"h264_ratecontrolmode"= cbr
s<0~(m-1)>_h2	framerate, imagequality	4/4	Set prioritypolicy
64_prioritypoli			* Only valid when
су			"h264_ratecontrolmode"= cbr
s<0~(m-1)>_h2	1~"capability_videoin_c<0	1/4	The maximum frame rates of a H264
64_maxframe	~(n-1)>_h264_maxframera		stream at different
	te"		resolutions("capability_videoin_c<0~(
			n-1)>_resolution") are recorded in
			"capability_videoin_c<0~(n-1)>_h264
			_maxframerate"
s<0~(m-1)>_h2	0~2	1/4	Indicate H264 profiles
64_profile			0: baseline
			1: main profile
			2: high profile
s<0~(m-1)>_h2	<boolean></boolean>	4/4	Enable "Smart Q" function.
64_smartq_en			* Only available when
able			"capability_videoin_c<0~(n-1)>_smart
			q_support" is 1.
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0309a.
s<0~(m-1)>_h2	<boolean></boolean>	4/4	Enable "Dynamic intra frame period".

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
65_dintraperio			* Only available when
d_enable			"capability_videoin_c<0~(n-1)>_dintra
			period_support" is 1 and h265 is listed
			in "capability_videoin_codec".
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0301c.
s<0~(m-1)>_h2	250, 500, 1000, 2000,	4/4	The time interval between two
65_intraperiod	3000, 4000		I-frames (Intra coded picture).
			The unit is millisecond (ms).
			* Only available when h265 is listed in
			"capability_videoin_codec".
s<0~(m-1)>_h2	cbr, vbr	4/4	cbr : Constant bit rate mode.
65_ratecontrol			vbr : Fixed quality mode, all frames are
mode			encoded in the same quality.
			* Only available when h265 is listed in
			"capability_videoin_codec".
s<0~(m-1)>_h2	1~5,	4/4	Set the pre-defined quality level:
65_quant	99, 100		1: Medium
			2: Standard
			3: Good
			4: Detailed
			5: Excellent
			100: Use the quality level in
			"qpercent"
			99: Use the quality level in "qvalue"
			* Only available when h265 is listed in
			"capability_videoin_codec" and
			"h265_ratecontrolmode"= vbr.
s<0~(m-1)>_h2	0~51	4/4	Manual video quality level input. The
65_qvalue			Q value which is used by encoded
			library directly.
			* Only available when h265 is listed in
			"capability_videoin_codec".
			* Only valid when
			"h265 ratecontrolmode"= vbr and

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			s<0~(m-1)>_h265_quant = 99.
s<0~(m-1)>_h2	1~100	4/4	Select customized quality in a
65_qpercent			normalized full range.
			1: Worst quality
			100: Best quality
			* Only available when h265 is listed in
			"capability_videoin_codec".
			* Only valid when
			"h265_ratecontrolmode"= vbr and
			"quant"= 100.
s<0~(m-1)>_h2	20000~"capability_videoin	4/4	The maximum allowed bit rate in fixed
65_maxvbrbitr	_c<0~(n-1)>_h265_maxbit		quality mode.
ate	rate"		When the bit rate exceeds this value,
			frames will be dropped to restrict the
			bit rate.
			* Only available when h265 is listed in
			"capability_videoin_codec".
			* Only valid when
			"h265_ratecontrolmode"= vbr
s<0~(m-1)>_h2	1~5, 100	4/4	Set the pre-defined quality level:
65_cbr_quant			1: Medium
			2: Standard
			3: Good
			4: Detailed
			5: Excellent
			100: Use the quality level in
			"cbr_qpercent"
			* Only available when h265 is listed in
			"capability_videoin_codec" and
			"h265_ratecontrolmode"= cbr.
			* Only available when
			"capability_smartstream_version" >=
			"2.0"
s<0~(m-1)>_h2	1~100	4/4	Select customized quality in a
65_cbr_qperce			normalized full range.
nt			1: Worst quality

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			100: Best quality
			* Only available when h265 is listed in
			"capability_videoin_codec".
			* Only valid when
			"h265_ratecontrolmode"= cbr and
			"quant"= 100.
			* Only available when
			"capability_smartstream_version" >=
			"2.0"
s<0~(m-1)>_h2	20000~"capability_videoin	4/4	The target bit rate in constant bit rate
65_bitrate	_c<0~(n-1)>_h265_maxbit		mode.
	rate"		* Only available when h265 is listed in
			"capability_videoin_codec".
			* Only valid when
			"h265_ratecontrolmode"= cbr
s<0~(m-1)>_h2	framerate, imagequality	4/4	Set prioritypolicy
65_prioritypoli			* Only available when h265 is listed in
су			"capability_videoin_codec".
			* Only valid when
			"h265_ratecontrolmode"= cbr
s<0~(m-1)>_h2	1~"capability_videoin_c<0	1/4	The maximum frame rates of a H265
65_maxframe	~(n-1)>_h265_maxframera		stream at different
	te"		resolutions("capability_videoin_c<0~(
			n-1)>_resolution") are recorded in
			"capability_videoin_c<0~(n-1)>_h265
			_maxframerate"
			* Only available when h265 is listed in
			"capability_videoin_codec".
s<0~(m-1)>_h2	Available values are listed	1/4	Indicate H265 profiles
65_profile	in "		* Only available when h265 is listed in
	capability_videoin_c<0~(n		"capability_videoin_codec".
	-1)>_h265_profile"		
s<0~(m-1)>_h2	<boolean></boolean>	4/4	Enable "Smart Q" function.
65_smartq_en			* Only available when h265 is listed in
able			"capability_videoin_codec".
			* Only available when

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			"capability_videoin_c<0~(n-1)>_smart
			q_support" is 1.
			* We support this parameter when
			the version number (httpversion) is
			equal or greater than 0309a.
s<0~(m-1)>_mj	cbr, vbr	4/4	cbr : Constant bit rate mode.
peg_ratecontr			vbr : Fixed quality mode, all frames are
olmode			encoded in the same quality.
s<0~(m-1)>_mj	1~5,	4/4	* Only valid when
peg_quant	99, 100		"mjpeg_ratecontrolmode"= vbr.
			Set the pre-defined quality level:
			1: Medium
			2: Standard
			3: Good
			4: Detailed
			5: Excellent
			100: Use the quality level in
			"qpercent"
			99: Use the quality level in "qvalue"
s<0~(m-1)>_mj	10~200	4/4	Manual video quality level input. The
peg_qvalue	(Only valid when		Q value which is used by encoded
	"capability_api_httpversio		library directly.
	n" format is XXXXX_1 or		* Only valid when
	XXXXX_3 or XXXXX_4		"mjpeg_ratecontrolmode"= vbr and
	ex: 0301a_1 or 0301a_3 or		s<0~(m-1)>_mjpeg_quant = 99
	0301a_4)		
	or 1~99		
	(Only valid when		
	"capability_api_httpversio		
	n" format is XXXXX_2,		
	ex: 0301a_2)		
	<product dependent=""></product>		
s<0~(m-1)>_mj	1~100	4/4	Select customized quality in a
peg_qpercent			normalized full range.
			1: Worst quality

NAME	VALUF	SECURITY(DESCRIPTION
		get/set)	
		8-99	100: Best quality
			* Only valid when
			"mipeg_ratecontrolmode"= vbr and
			$s<0^{(m-1)}$ mipeg quant = 100.
s<0~(m-1)> mj	20000~"capability videoin	4/4	The maximum allowed bit rate in fixed
peg maxvbrbit	c<0~(n-1)> mjpeg maxbi		guality mode.
rate	trate"		When the bit rate exceeds this value,
			frames will be dropped to restrict the
			bit rate.
			* Only valid when
			"mjpeg_ratecontrolmode"= vbr
s<0~(m-1)>_mj	1~5, 100	4/4	Set the pre-defined quality level:
peg_cbr_quant			1: Medium
			2: Standard
			3: Good
			4: Detailed
			5: Excellent
			100: Use the quality level in
			"cbr_qpercent"
			* Only valid when
			"mjpeg_ratecontrolmode"= cbr.
			* Only available when
			"capability_smartstream_version" >=
			"2.0"
s<0~(m-1)>_mj	1~100	4/4	Select customized quality in a
peg_cbr_qperc			normalized full range.
ent			1: Worst quality
			100: Best quality
			* Only valid when
			"mjpeg_ratecontrolmode"= cbr and
			"quant"= 100.
			* Only available when
			"capability_smartstream_version" >=
			"2.0"
s<0~(m-1)>_mj	20000~"capability_videoin	4/4	The target bit rate in constant bit rate
peg_bitrate	_c<0~(n-1)>_mjpeg_maxbi		mode.

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
	trate"		* Only valid when
			"mjpeg_ratecontrolmode"= cbr
s<0~(m-1)>_mj	framerate, imagequality	4/4	Set prioritypolicy
peg_prioritypo			* Only valid when
licy			"mjpeg_ratecontrolmode"= cbr
s<0~(m-1)>_mj	1~"capability_videoin_c<0	1/4	The maximum frame rates of a mjpeg
peg_maxframe	~(n-1)>_mjpeg_maxframer		stream at different
	ate"		resolutions("capability_videoin_c<0~(
			n-1)>_resolution") are recorded in
			"capability_videoin_c<0~(n-1)>_mjpe
			g_maxframerate"
s<0~(m-1)>_ra	<boolean></boolean>	1/4	Change resolution to fit 4:3 ratio.
tiocorrect			For PAL:
			D1/4ClF(720/704x576) -> (768x576)
			CIF(352x288)->(384x288)
			For NTSC:
			D1/4CIF(720/704x480) -> (640x480)
			CIF(352x240)->(320x240)
			* Only available when
			capability_videoin_type is 0 or 1.
wdrpro_mode	<boolean></boolean>	4/4	Enable WDR pro
<product< td=""><td></td><td></td><td>* Only available when</td></product<>			* Only available when
dependent>			"capability_image_c<0~(n-1)>_wdrpro
			_mode" > 0
wdrpro_streng	1~100	4/4	The strength of WDR Pro.
th			The bigger value means the stronger
<product< td=""><td></td><td></td><td>strength of WDR Pro.</td></product<>			strength of WDR Pro.
dependent>			* Only available when
			"capability_image_c<0~(n-1)>_wdrpro
			_strength" is 1
wdrc_mode	<boolean></boolean>	4/4	Enable WDR enhanced.
<product< td=""><td></td><td></td><td>* Only available when</td></product<>			* Only available when
dependent>			"capability_image_c<0~(n-1)>_wdrc_
			mode" is 1
wdrc_strength	1~100	4/4	The strength of WDR enhanced.
<product< td=""><td></td><td></td><td>The bigger value means the stronger</td></product<>			The bigger value means the stronger

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
dependent>			strength of WDR enhanced.
			* Only available when
			"capability_image_c<0~(n-1)>_wdrc_
			mode" is 1
aespeed_mod	<boolean></boolean>	4/4	Turning AE converge speed on or off.
e			0: off
<product< td=""><td></td><td></td><td>1: on</td></product<>			1: on
dependent>			* Only available when
			"capability_image_c<0~(n-1)>_aespee
			d" is 1
aespeed_spee	1~100	4/4	The speed level of AE converge speed.
dlevel			1~20: level 1
<product< td=""><td></td><td></td><td>21~40: level 2</td></product<>			21~40: level 2
dependent>			41~60: level 3
			61~80: level 4
			81~100: level 5
			Level 1~4(low ~ high)
			The higher speed level meas shorter
			AE converged time during AE
			executing.
			* Only available when
			"capability_image_c<0~(n-1)>_aespee
			d" is 1
aespeed_sensi	1~100	4/4	The sensitivity of AE converge speed.
tivity			1~20: level 1
<product< td=""><td></td><td></td><td>21~40: level 2</td></product<>			21~40: level 2
dependent>			41~60: level 3
			61~80: level 4
			81~100: level 5
			Level 1~4(low ~ high)
			The higher sensitivity level meas that
			it is easy to be trigger while scene
			changed.
			* Only available when
			"capability_image_c<0~(n-1)>_aespee
			d" is 1 and

NAME	VALUE	SECURITY(DESCRIPTION
		get/set)	
			"capability_image_c<0~(n-1)>_aespee
			dsupportsensitivity" is 1.
flickerless	<boolean></boolean>	4/4	Turn on(1) or turn off(0) the flickerless
<product< td=""><td></td><td></td><td>mode</td></product<>			mode
dependent>			* Only available when
			"capability_image_c<0~(n-1)>_flickerl
			ess" is 1.
mounttype	ceiling, wall, floor	1/6	Hardware installation.
			* Only available when
			"capability_videoin_c<0~(n-1)>_moun
			ttype" != "-".
enablewaterm	0, 1	1/6	0: Not to add watermarks on images
ark			1: Add watermarks on images
<product< td=""><td></td><td></td><td>* Only available when</td></product<>			* Only available when
dependent>			"capability_fisheye" > 0
s<0~(m-2)>_fis	'10, 1P, 2P, 1R, 4R' for	1/4	Local dewarp mode.
heyedewarpm	ceiling/floor mount		"10" is original mode (disable).
ode	'10, 1P, 1R, 4R' for wall		Supported dewarp mode is different
<product< td=""><td>mount</td><td></td><td>by mount type.</td></product<>	mount		by mount type.
dependent>	<product dependent=""></product>		(videoin_c<0~(n-1)>_mounttype)
			Supported mode list could be
			extracted from
			(capability_videoin_c<0~(n-1)>_locald
			ewarp_typeceilingmount) and
			(capability_videoin_c<0~(n-1)>_locald
			ewarp_typewallmount)
			* Only available when
			"capability_fisheyelocaldewarp_c<0~(
			capability_nvideoin)-1>" > 0

Group: videoin_c<0~(n-1)>_s<0~(m-1)>_h264_smartstream2 (capability_smartstream_support=1 and capability_smartstream_version>=2.0)

Group: videoin_c<0~(n-1)>_s<0~(m-1)>_h265_smartstream2 (capability_smartstream_support=1, capability_smartstream_version>=2.0 and h265 is listed in "capability_videoin_codec") n denotes the value of "capability_nvideoin", m denotes the value of " capability_nmediastream"