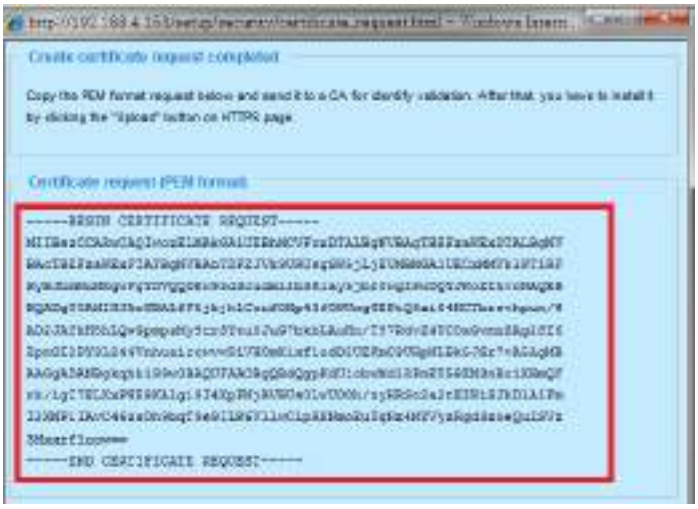
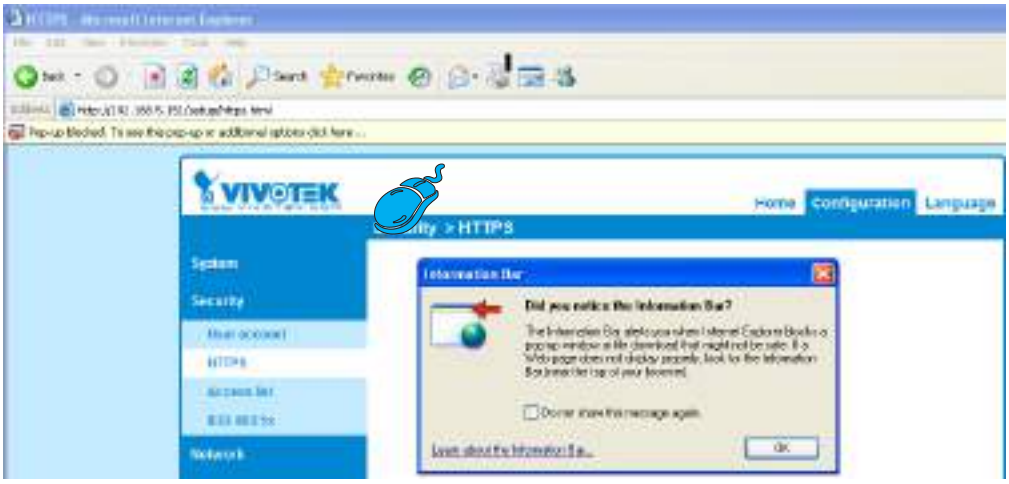
Create certificate request and install

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.

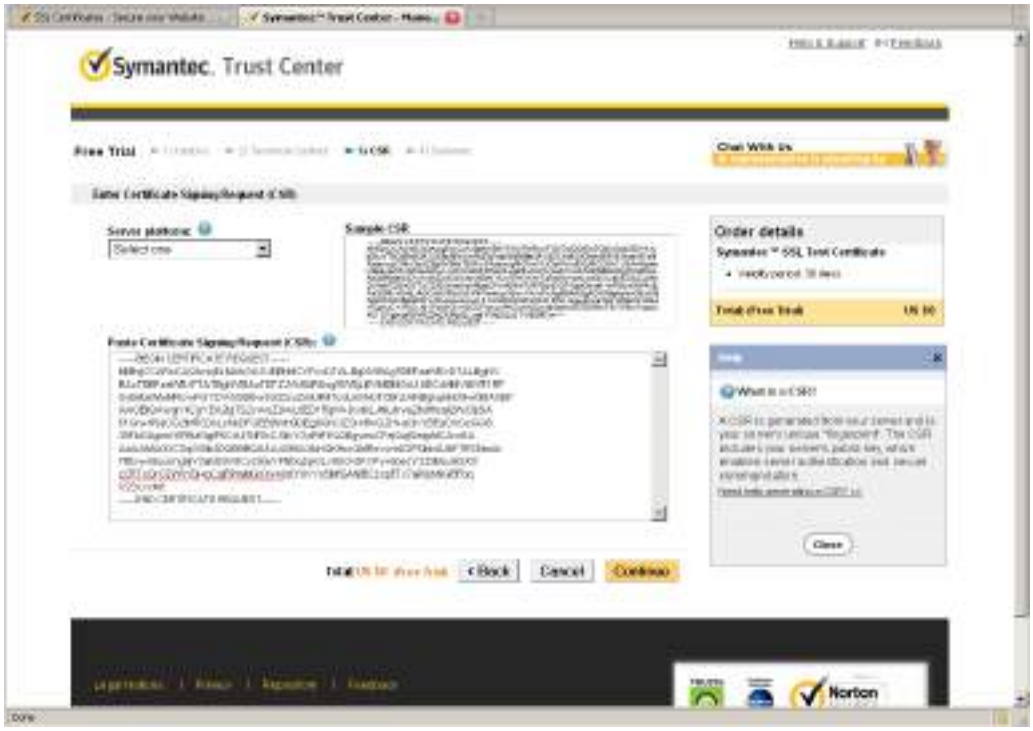
4. The Certificate request window will prompt.



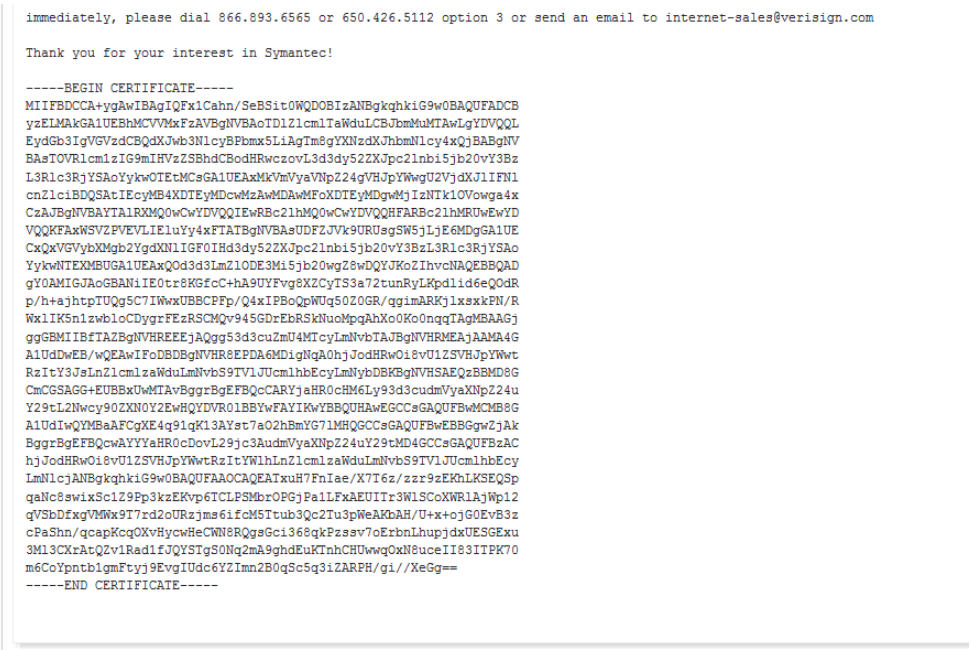
If you see the following Information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.



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.

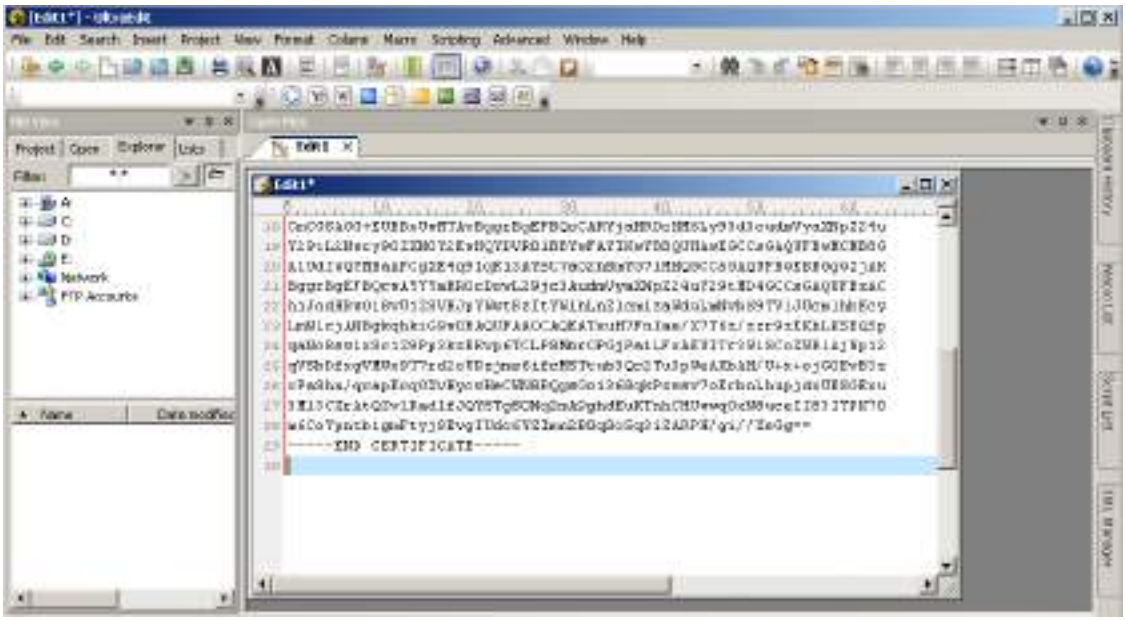


6. Once completed, your SSL certificate should be delivered to you via an email or other means. Copy the contents of the certificate in the email and paste it in a text/HTML/hex editor/converter, such as IDM Computer Solutions' UltraEdit.

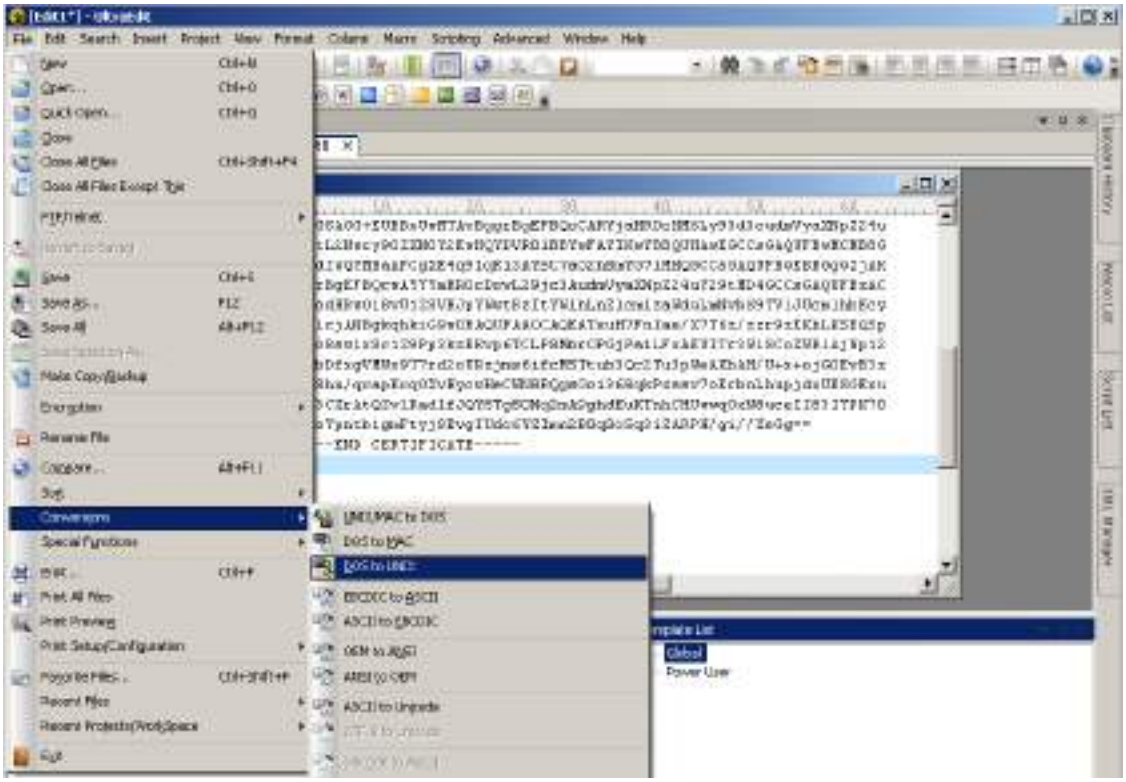


```
immediately, please dial 866.893.6565 or 650.426.5112 option 3 or send an email to internet-sales@verisign.com

Thank you for your interest in Symantec!

-----BEGIN CERTIFICATE-----
MIIFBDCCA+ygAwIBAgIQFx1Cahn/SeBSit0WQDOBIzANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwOTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFN1
cnZlciBDQSAtIEcyMB4XDTEyMDcwMzAwMDAwMFoXDTEyMDgwMjIzNTk1OVowga4x
CzAJBgNVBAYTAlRXMQ0wCwYDVQQIEwRBc2lhMQ0wCwYDVQQHFARBc2lhMRUwEwYD
VQQKFAxWSVZPVEVLIEluYy4xFTATBgNVBAsUDFZJVk9URUsgSW5jLjE6MDgGA1UE
CxQxVGVybXMgb2YgdXNlIGF0IHd3dy52ZXJpc2lnbi5jb20vY3BzL3Rlc3RjYSAo
YykwNTEXMBUGA1UEAxQOd3d3LmZlODE3Mi5jb20wgZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBANiIE0tr8KGfcC+hA9UYFvg8XZCyTS3a72tunRyLKpdlid6eQOdR
p/h+ajhtpTUQg5C7IWwxUBBCPFp/Q4xIPBoQpWUq50Z0GR/qgimARKjlxsxkPN/R
WxlIK5n1zwbloCDygrFEzRSCMQv945GDrEbRSkNuoMpqAhXo0Ko0nqqTAgMBAAGj
ggGBMIIBfTAZBgNVHREEEjAQgg53d3cuZmU4MTcyLmNvbTAJBgNVHRMEAjAAMA4G
A1UdDwEB/wQEAwIFoDBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSVHJpYWwt
RzItY3JsLnZlcmlzaWduLmNvbS9TVlJUcmlhbEcyLmNybDBKBgNVHSAEQzBBMD8G
CmCGSAGG+EUBBxUwMTAvBggrBgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24u
Y29tL2Nwcy90ZXN0Y2EwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB8G
A1UdIwQYMBaAFCgXE4q91qK13AYst7aO2hBmYG7lMHQGCCsGAQUFBwEBBGgwZjAk
BggrBgEFBQcwAYYYaHR0cDovL29jc3AudmVyaXNpZ24uY29tMD4GCCsGAQUFBzAC
hjJodHRwOi8vU1ZSVHJpYWwtRzItYWlhLnZlcmlzaWduLmNvbS9TVlJUcmlhbEcy
LmNlcjANBgkqhkiG9w0BAQUFAAOCAQEATxuH7FnIae/X7T6z/zzr9zEKhLKSEQSp
qaNc8swixSc1Z9Pp3kzEKvp6TCLPSMbrOPGjPa1LFxAEUITr3WlSCoXWRlAjWp12
qVSbDfxgVMWx9T7rd2oURzjms6ifcM5Ttub3Qc2Tu3pWeAKbAH/U+x+ojG0EvB3z
cPaShn/qcapKcqOXvHycwHeCWN8RQgsGci368qkPzssv7oErbnLhupjdxUESGExu
3Ml3CXrAtQZv1Rad1fJQYSTgS0Nq2mA9ghdEuKTnhCHUwwqOxN8uceII83ITPK70
m6CoYpntb1gmFtyj9EvgIUdc6YZImn2B0qSc5q3iZARPH/gi//XeGg==
-----END CERTIFICATE-----
```

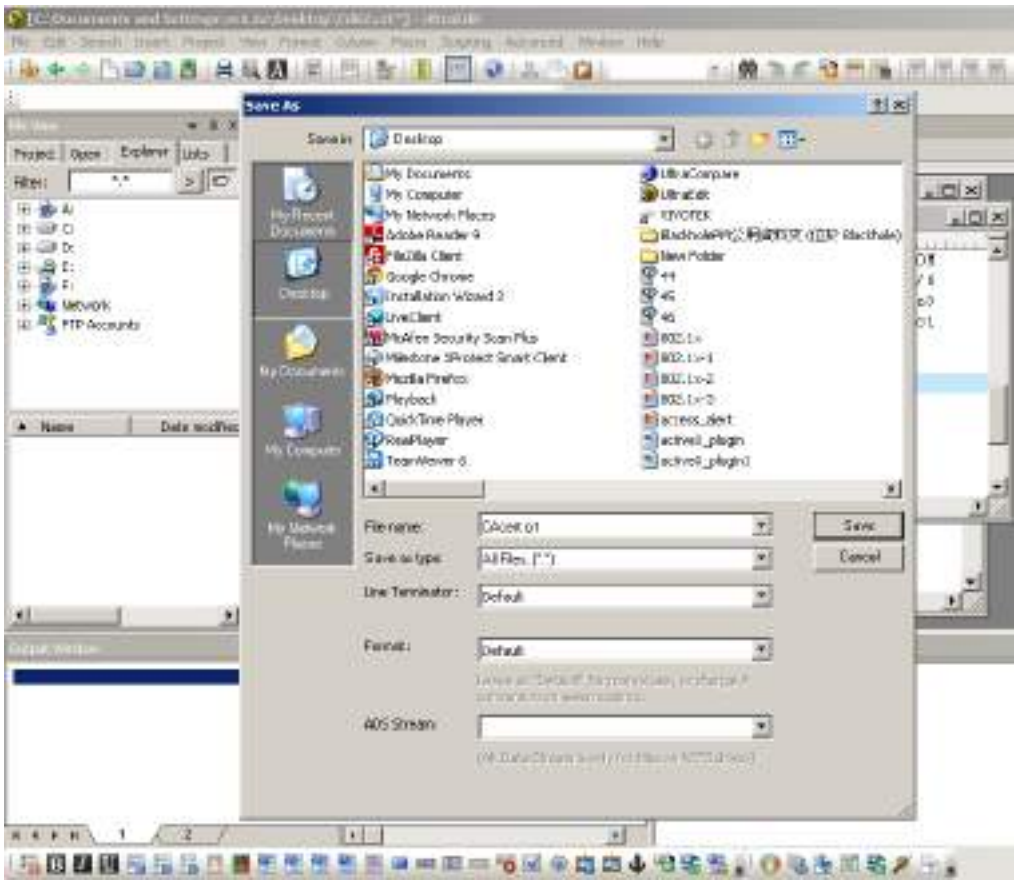
7. Open a new edit, paste the certificate contents, and press ENTER at the end of the contents to add an empty line.



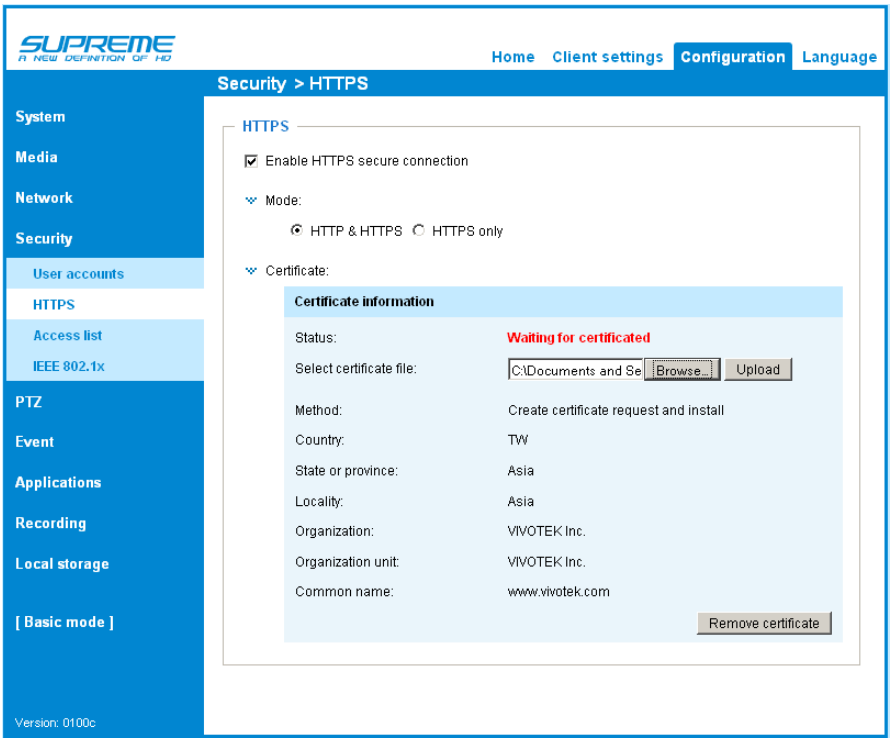
8. Convert file format from DOS to UNIX. Open **File** menu > **Conversions** > **DOS to Unix**.



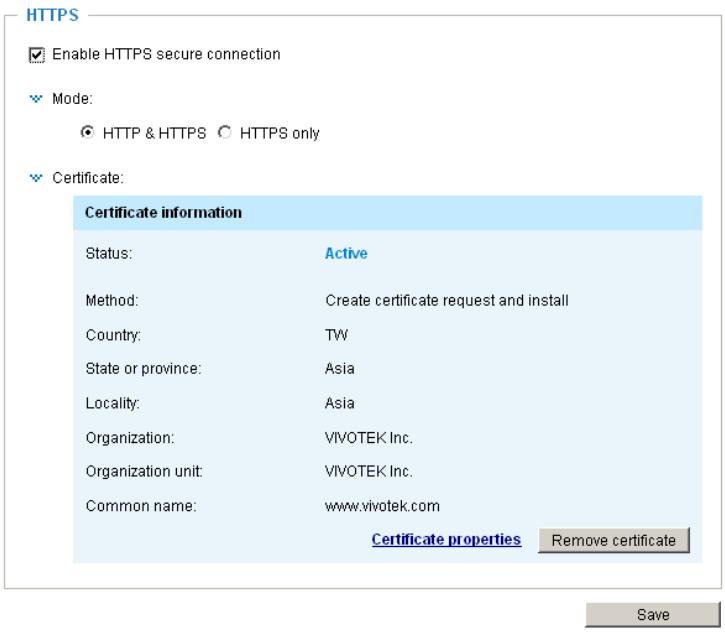
9. Save the edit using the “.crt” extension, using a file name like “CAcert.crt.”



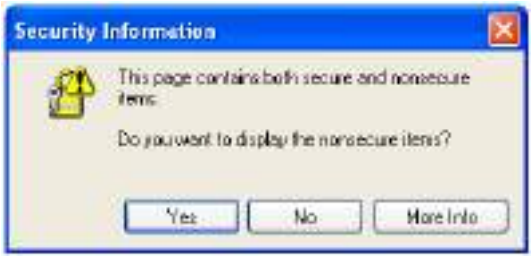
10. Return to the original firmware session, use the **Browse** button to locate the crt certificate file, and click **Upload** to enable the certification.



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.



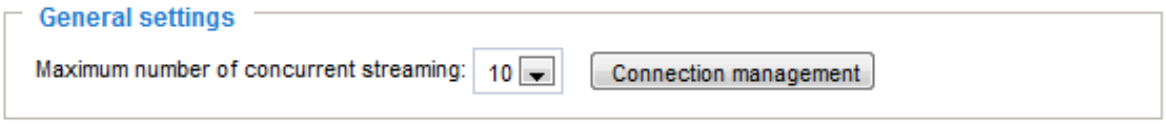
12. To begin an encrypted HTTPS session, click **Home** to return to the main page. Change the URL address from "http://" to "https://" in the address bar and press **Enter** on your keyboard. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.



Security > Access List

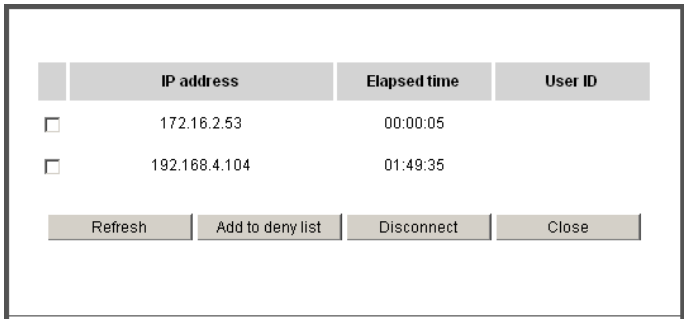
This section explains how to control access permission by verifying the client PC's IP address.

General Settings



Maximum number of concurrent streaming connection(s) limited to: 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).

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



	IP address	Elapsed time	User ID
☐	172.16.2.53	00:00:05	
☐	192.168.4.104	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

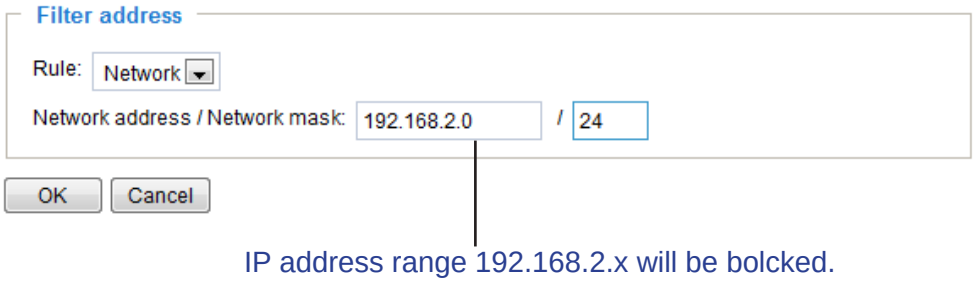
Enable access list filtering: Check this item and click **Save** if you want to enable the access list filtering function.

Filter type: 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.

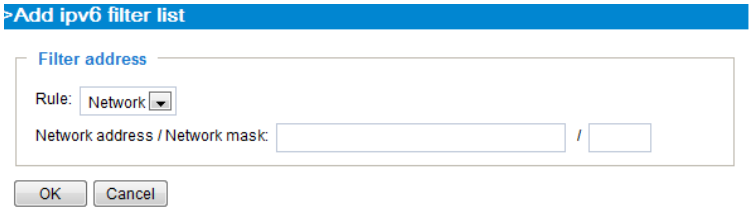
Then you can **Add** a rule to the following Access List. Please note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about **IPv6 Settings**, please refer to Network > General settings on page 81 for detailed information.

There are three types of rules:
Single: This rule allows the user to add an IP address to the Allowed/Denied list.
For example:

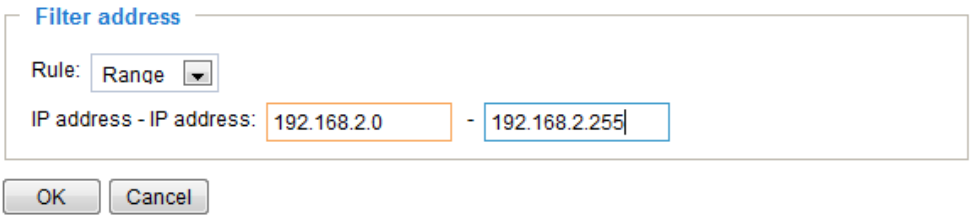
Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List. The address and network mask are written in CIDR format.
For example:



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.

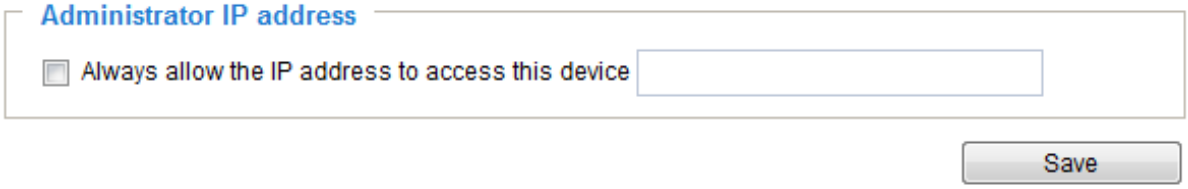


Range: This rule allows the user to assign a range of IP addresses to the Allow/Deny List.
Note: This rule only applies to IPv4 addresses.
For example:



Administrator IP address

Always allow the IP address to access this device: 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.



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:

Supplicant
(Network Camera)

Authenticator
(Network Switch)

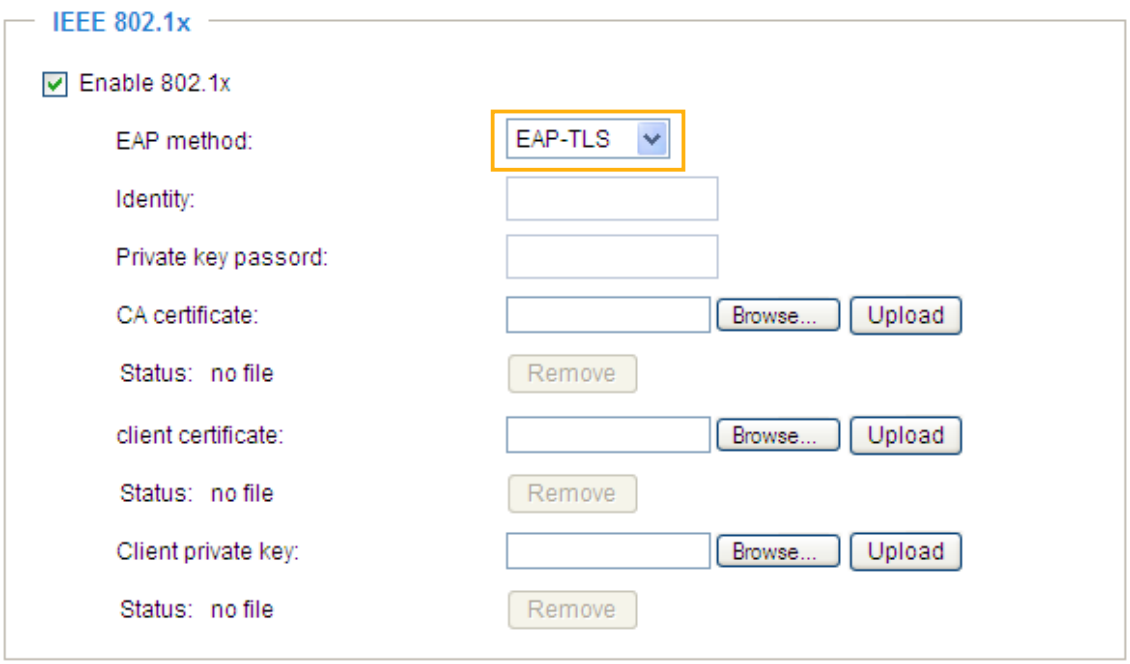
Authentication Server
(RADIUS Server)

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.
2. Connect the Network Camera to a PC or notebook outside of the protected LAN. Open the configuration page of the Network Camera as shown below. Select **EAP-PEAP** or **EAP-TLS** as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).

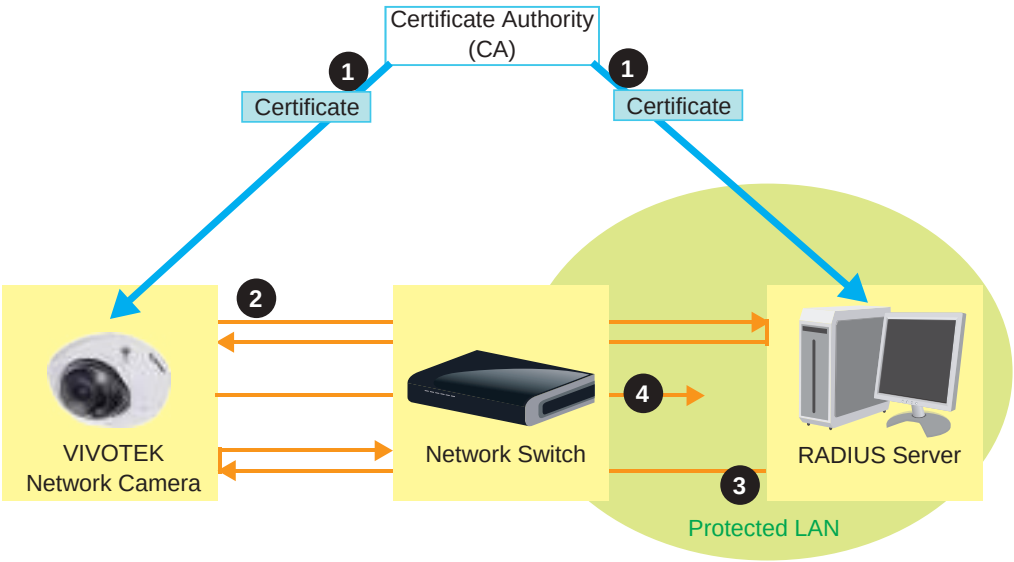


3. When all settings are complete, move the Network Camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

NOTE:

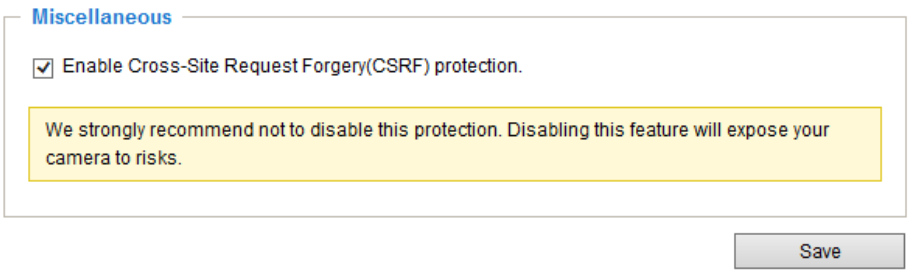
► *The authentication process for 802.1x:*

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.



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:

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.

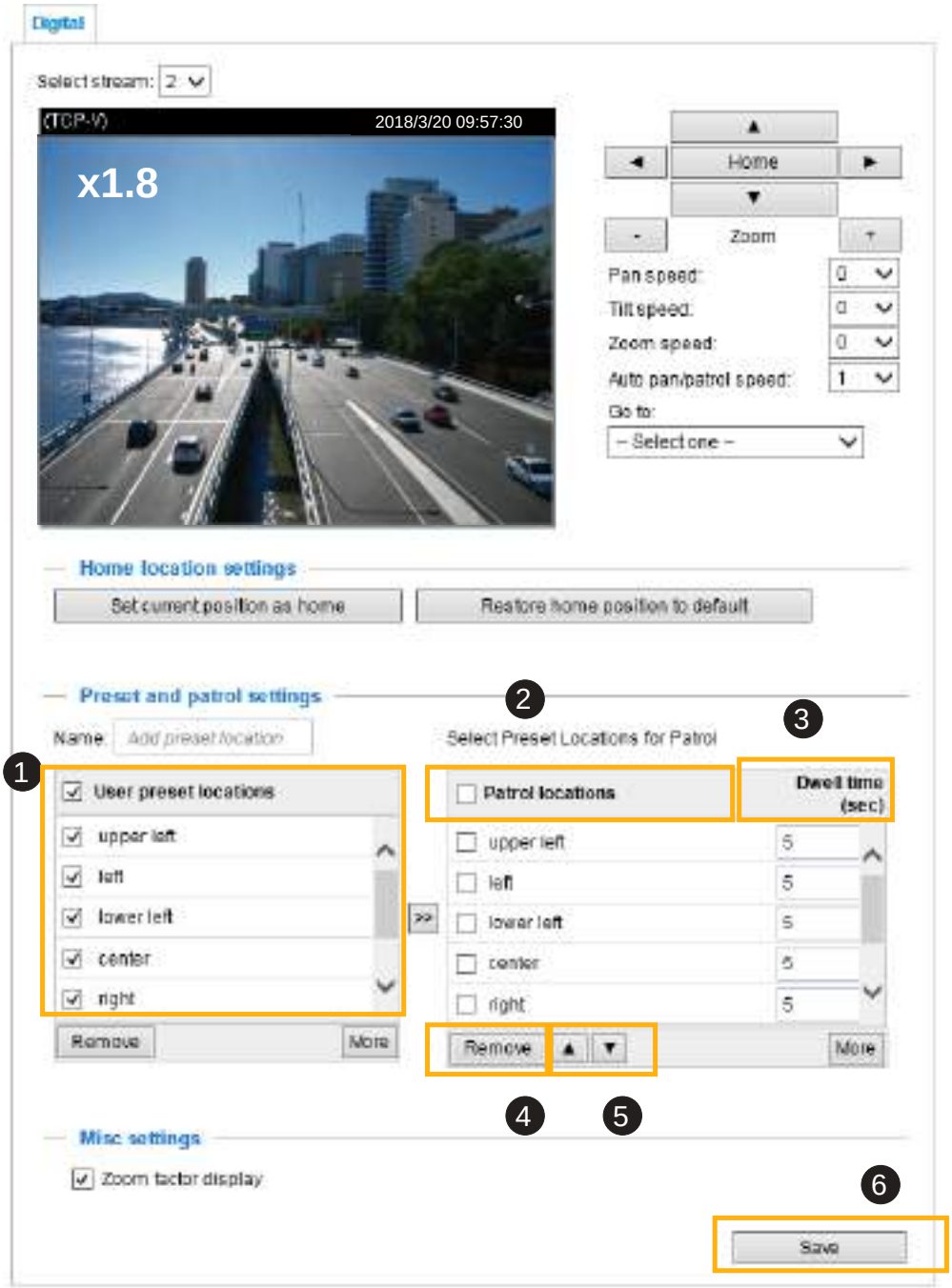
Note that the”Click on Image” function only applies when you have configured a smaller “Region of Interest” out of the maximum output frame! e.g., an 800 x 600 region from out of the camera’s maximum frame size.

Patrol button: 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 [>>].
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 [▲] [▼] 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.

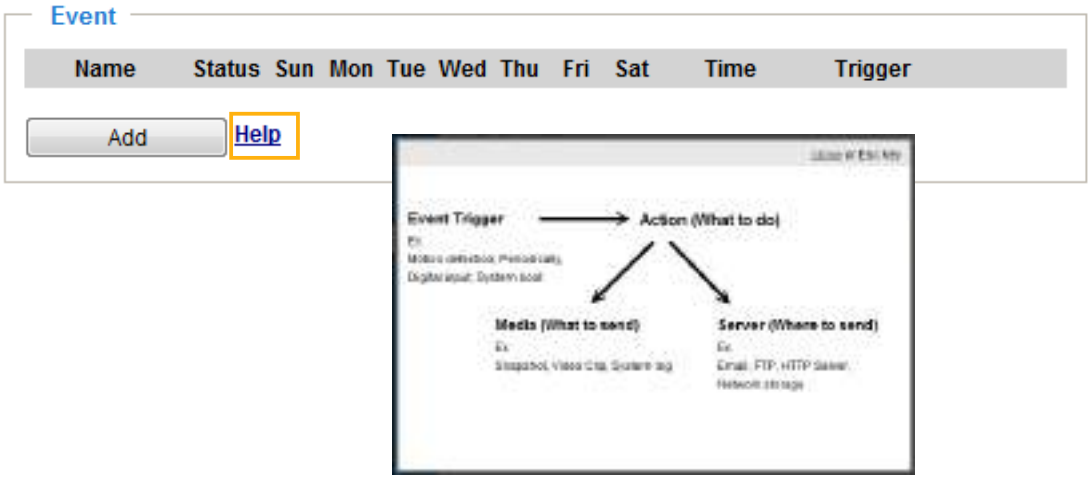


NOTE:

- 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.

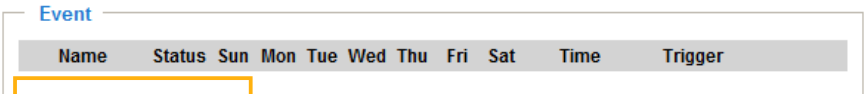
Event > Event settings

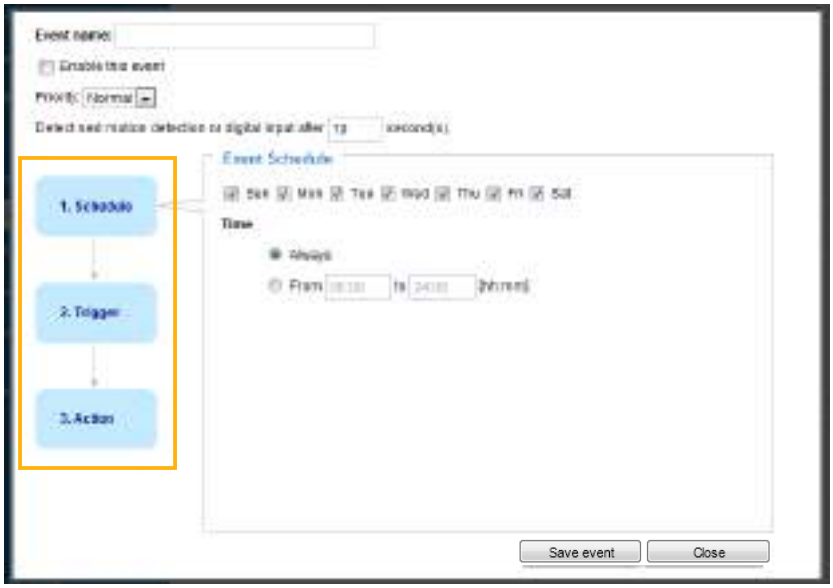
This section explains how to configure the Network Camera to respond to particular situations (event). A typical application is that when a motion is detected, the Network Camera sends buffered images to an FTP server or e-mail address as notifications. Click on **Help**, there is an illustration shown 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.



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: 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 ☐ 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

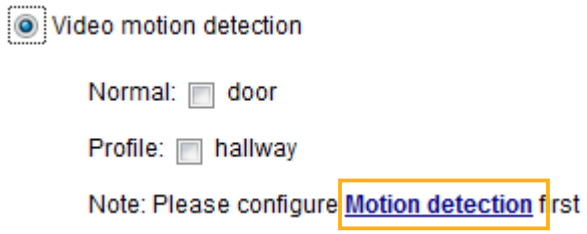
Specify the period of time during which the event trigger will take effect. Please select the days of the week and the time in a day (in 24-hr time format) for the event triggering schedule. For example, you may prefer an event to be triggered only during the off-office hours.

2. Trigger

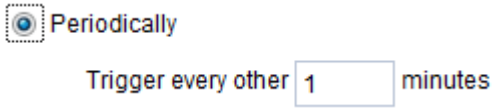
This is the cause or stimulus which defines when to trigger the Network Camera. The trigger source can be configured to use the Network Camera's built-in motion detection mechanism or external digital input devices.

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.



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



■ 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.

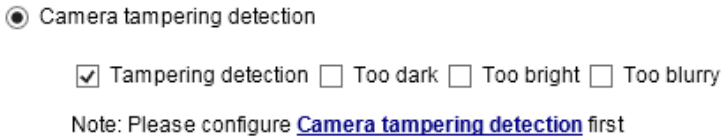
■ Recording notify
This option allows the Network Camera to trigger when the recording disk is full or when recording starts to overwrite older data.

■ 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.

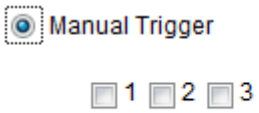
■ Camera tampering detection

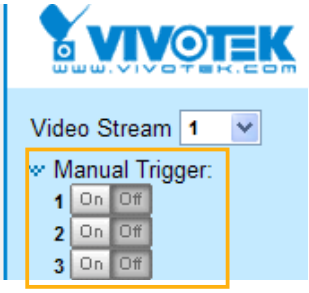
This option allows the Network Camera to trigger when the camera detects that is is being tampered with. To enable this function, you need to configure the Tampering Detection option first. Please refer to page 137 for detailed information.



■ 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.

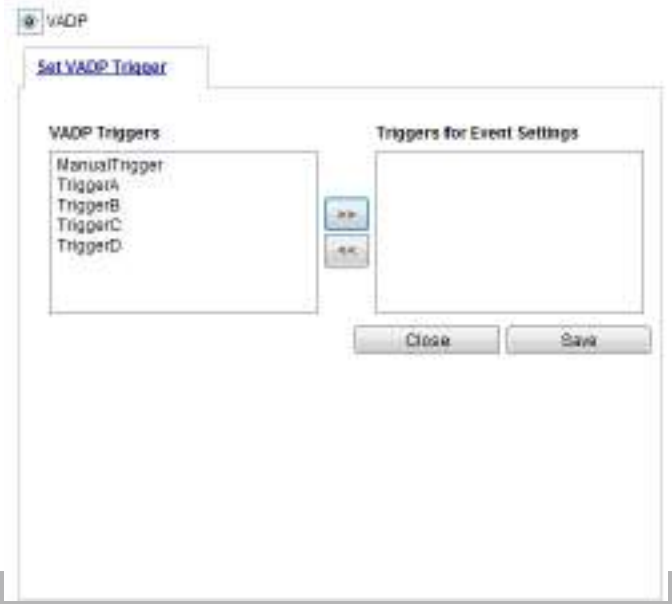




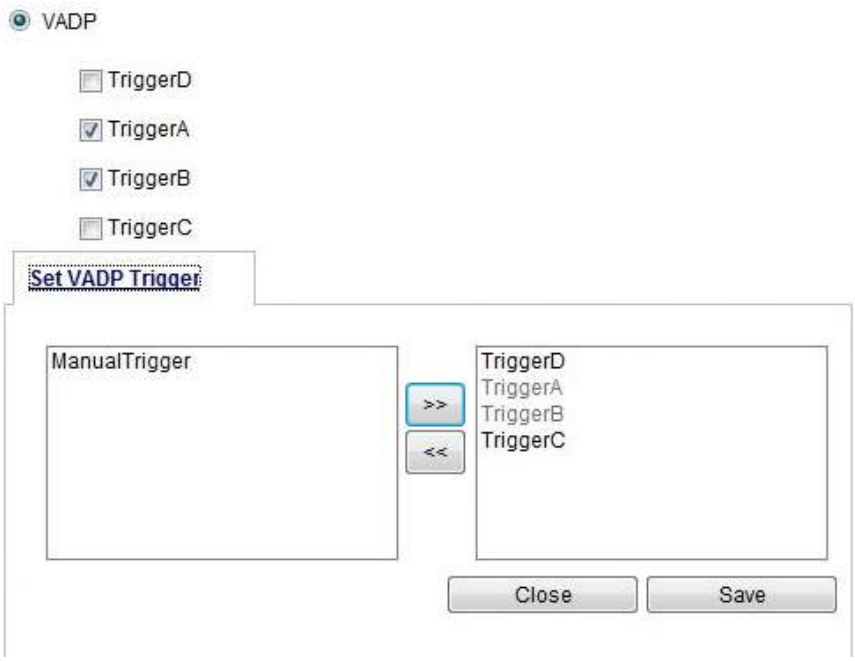
■ VADP

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.

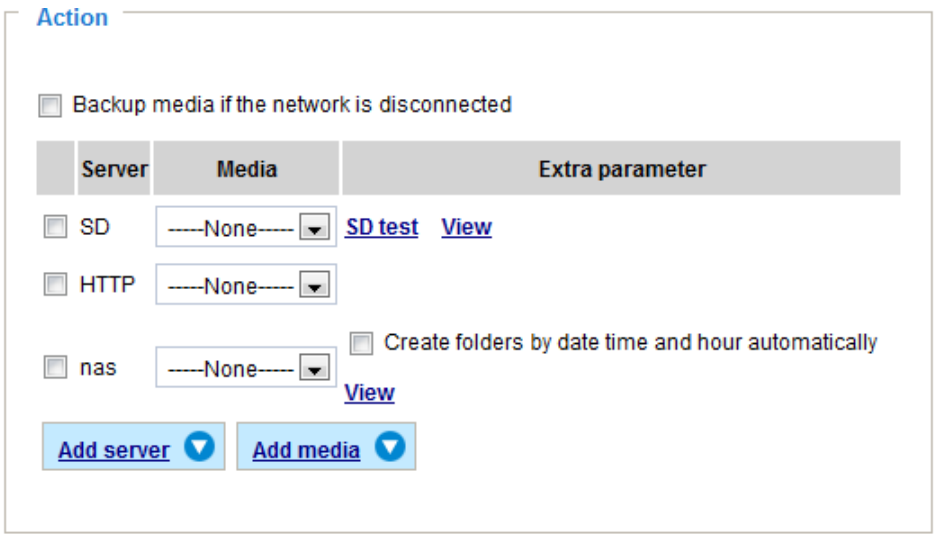


Once the triggers are configured, they will be listed under the VADP option.



3. Action

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



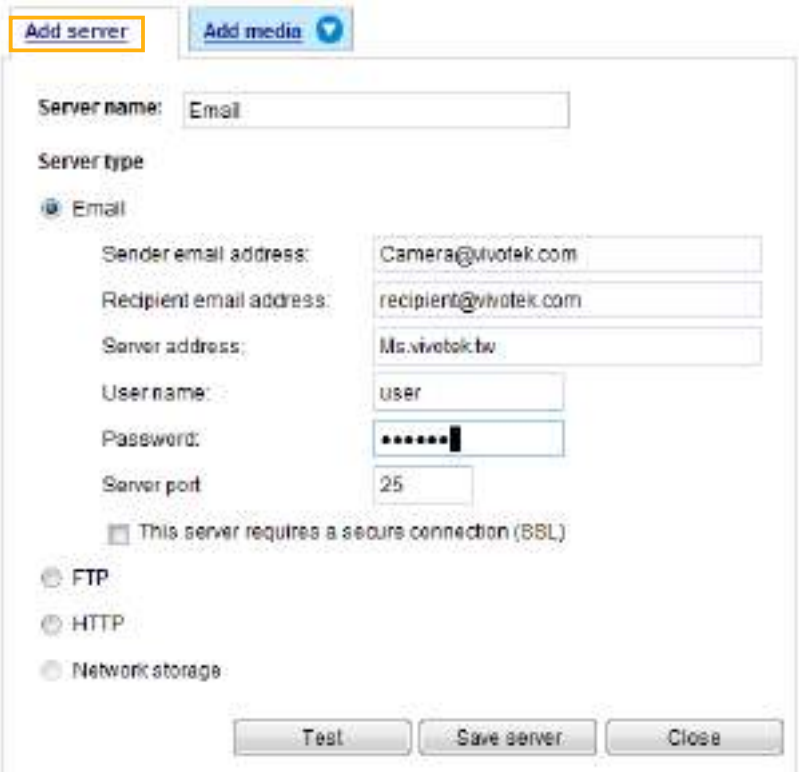
■ Backup media if the network is disconnected

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.



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.

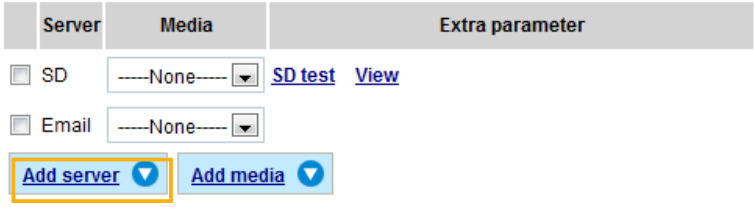
■ Server port: The default mail server port is set to 25. You can also manually set another port.

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.

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 type - FTP

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

■ 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.

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

<u>Server type - HTTP</u>

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

■ 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.

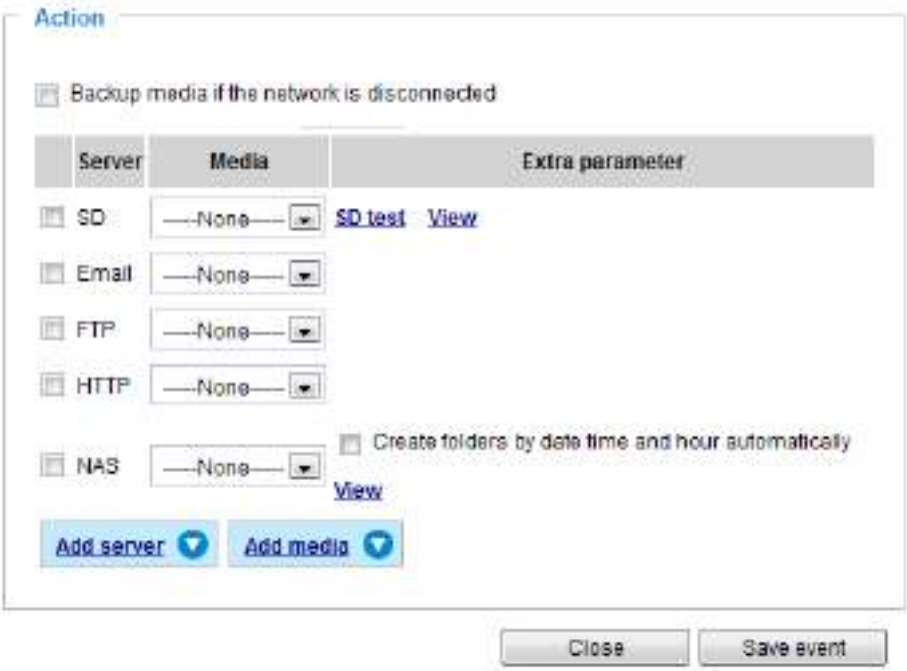
■ Password: Enter the password if necessary.

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.

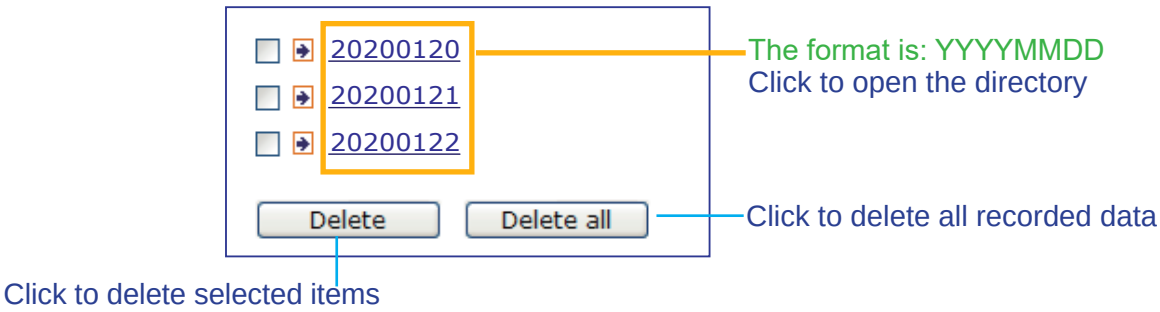


- SD Test: Click to test your SD card. The system will display a message indicating the result as a success or a failure. If you want to use your SD card for local storage, please format it before use. Please refer to page 128 for detailed information.

- 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 **20200120** to open the directory:

The format is: HH (24r)
Click to open the file list for that hour

< 07 08 09 10 11 12 13 14 15 16 17 >

	file name	size	date	time
☐	Recording1_58.mp4	2526004	2020/01/20	07 58 28
☐	Recording1_59.mp4	2563536	2020/01/20	07 59 28

Delete | Delete all | Back

Click to delete selected items

Click to delete all recorded data

Click to go back to the previous level of the directory

< 07 08 09 10 11 12 13 14 15 16 17 >

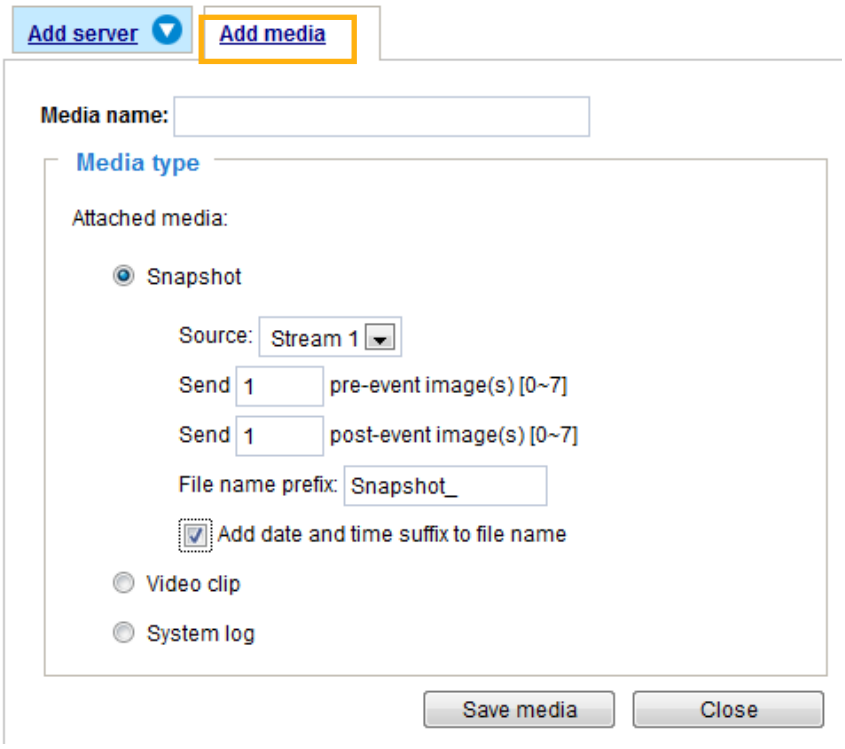
	file name	size	date	time
☐	Recording1_58.mp4	2526004	2020/01/20	07:58:28
☐	Recording1_59.mp4	2563536	2020/01/20	07:59:28

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.



Media type - Snapshot
Select to send snapshots when a trigger is activated.

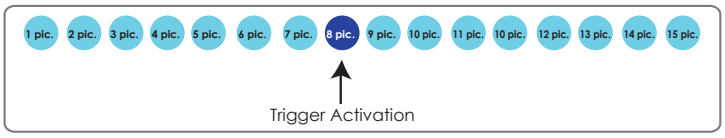
■ Media name: Enter a name for the media setting.

■ 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.



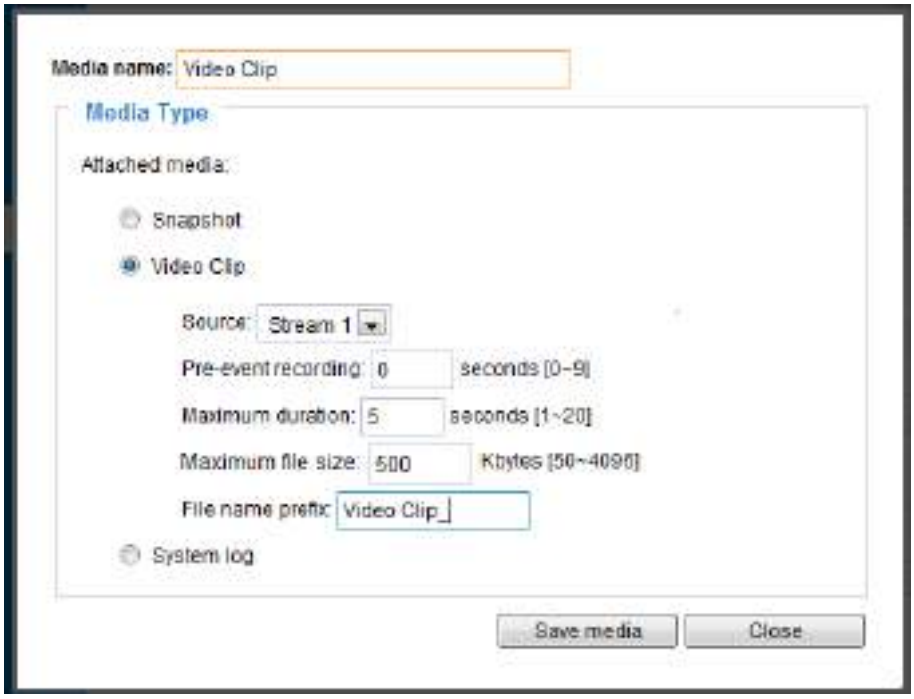
■ File name prefix
Enter the text that will be appended to the front of the file name.

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

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.

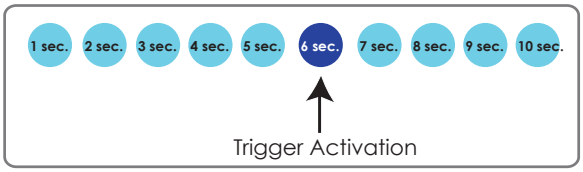


■ Media name: Enter a name for the media setting.

■ Source: Select a video stream as the source of video clip.

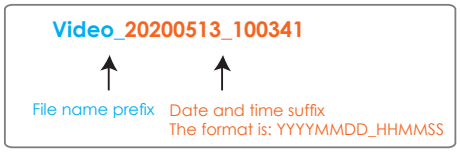
■ Pre-event recording
The Network Camera has a buffer to temporarily hold data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

■ 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.



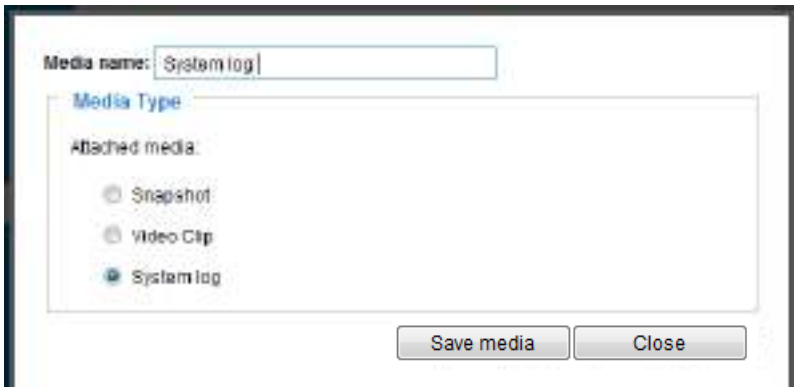
■ Maximum file size
Specify the maximum file size allowed. Some users may need to stitch the video clips together when searching and packing up forensic evidence.

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

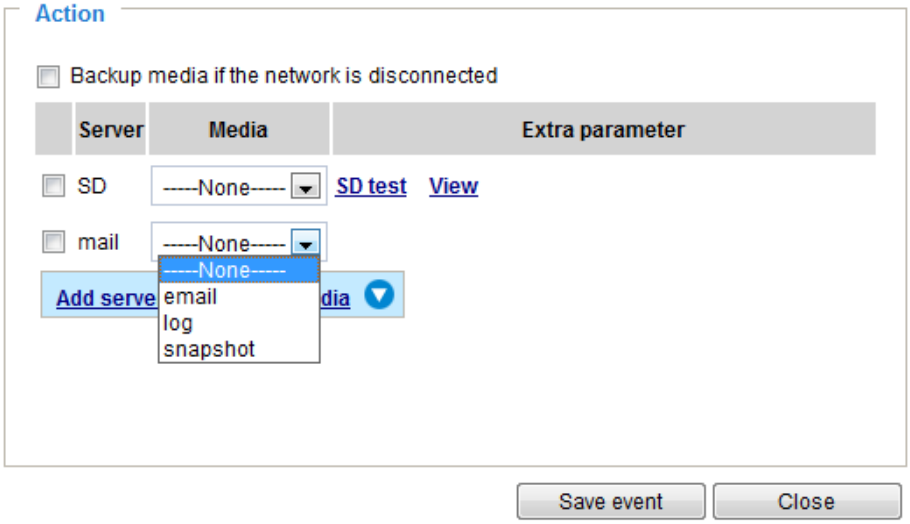


Click **Save media** to enable the settings.

Media type - System log
Select to send a system log when a trigger is activated.



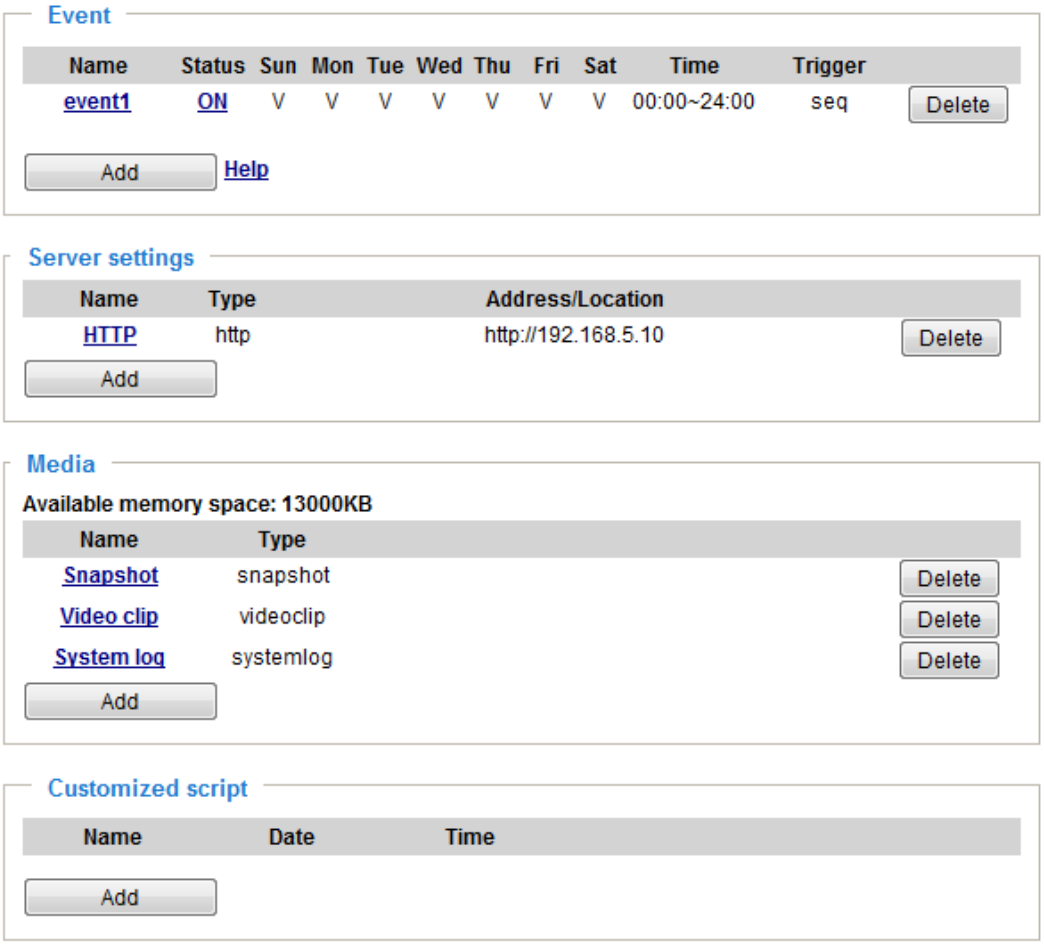
Click **Save media** to enable the settings, then click **Close** to exit the page.



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.

Please see the example of the Event setting page below:



When the Event Status is **ON**, the event configuration above is triggered by motion detection, the Network Camera will automatically send snapshots via e-mail.

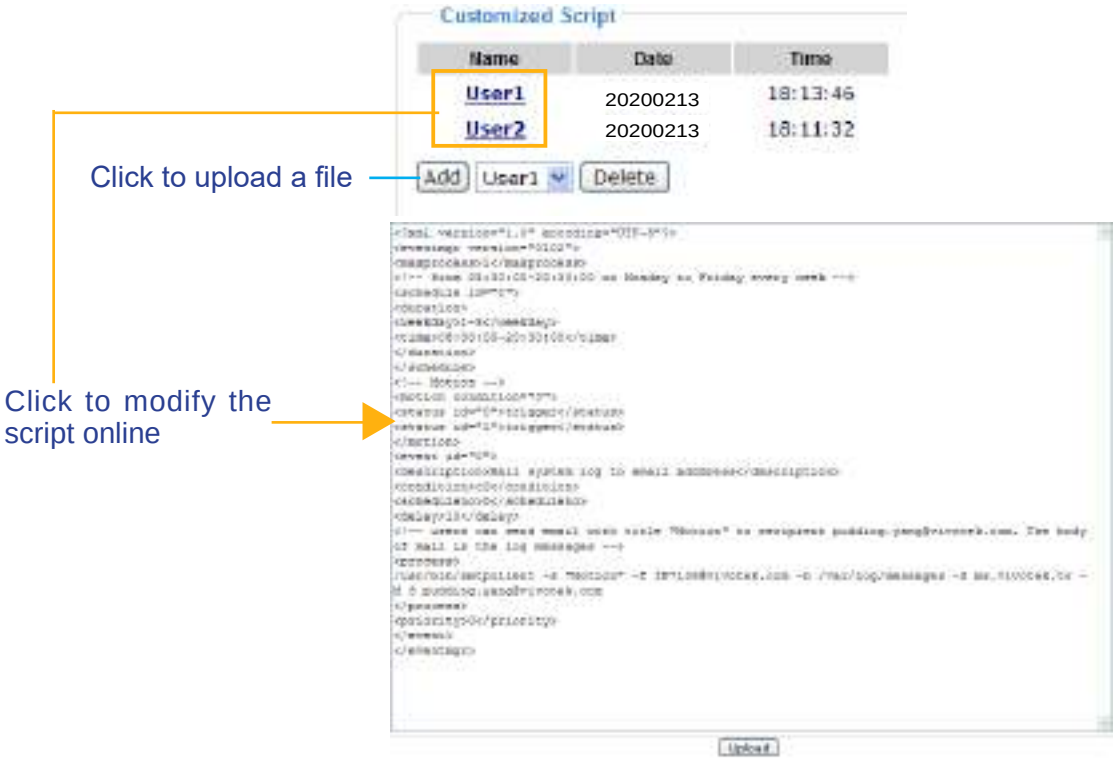
If you want to stop the event trigger, you can click on the **ON** button to turn it to **OFF** status or click the **Delete** button to remove the event setting.

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.

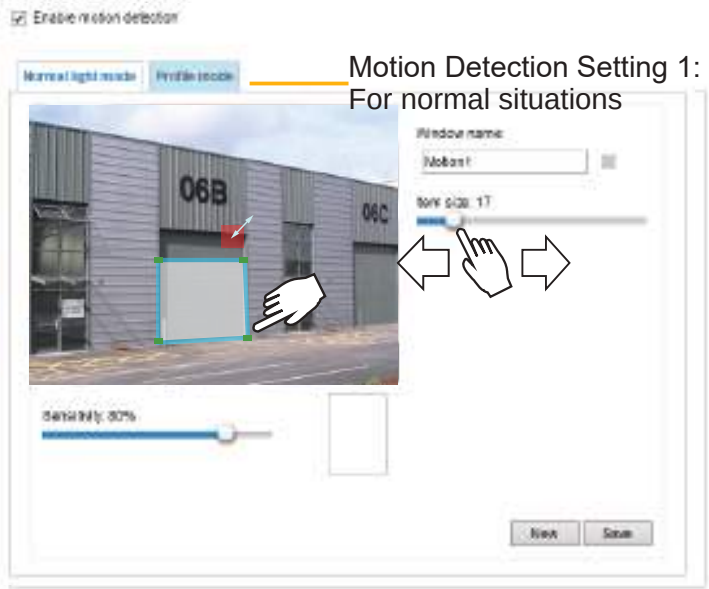
Customized Script

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:

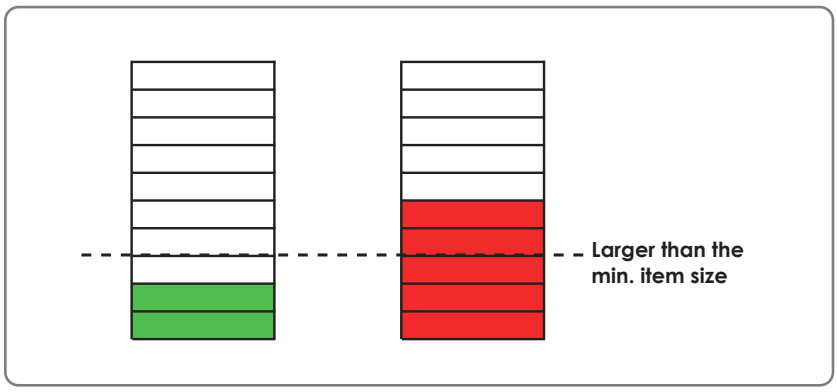
1. Click **New** to add a new motion detection window.
2. In the Window Name text box, enter a name for the motion detection window.
   - Use 4 mouse clicks to designate a detection window. You can change the window shape by dragging the corner marks to a preferred location.
   - Drag the item size tab 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.

For example:

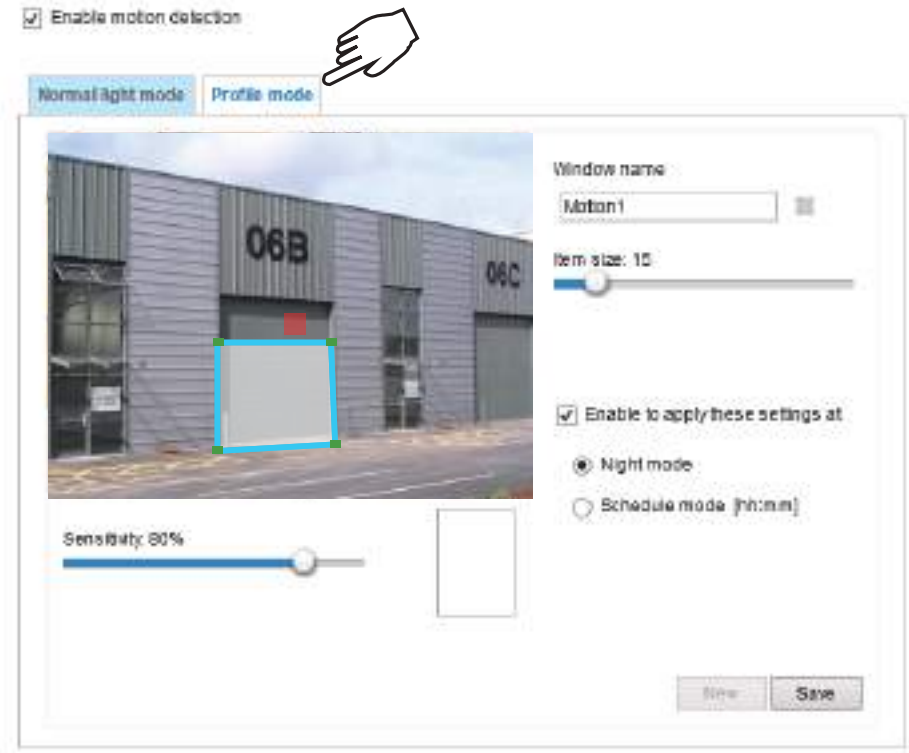
The Percentage Indicator will rise or fall depending on the variation between sequential images. When motions are detected by the Network Camera and are considered to exceed the preset threshold, the red bar rises. Meanwhile, the motion detection window will be outlined in red.

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.

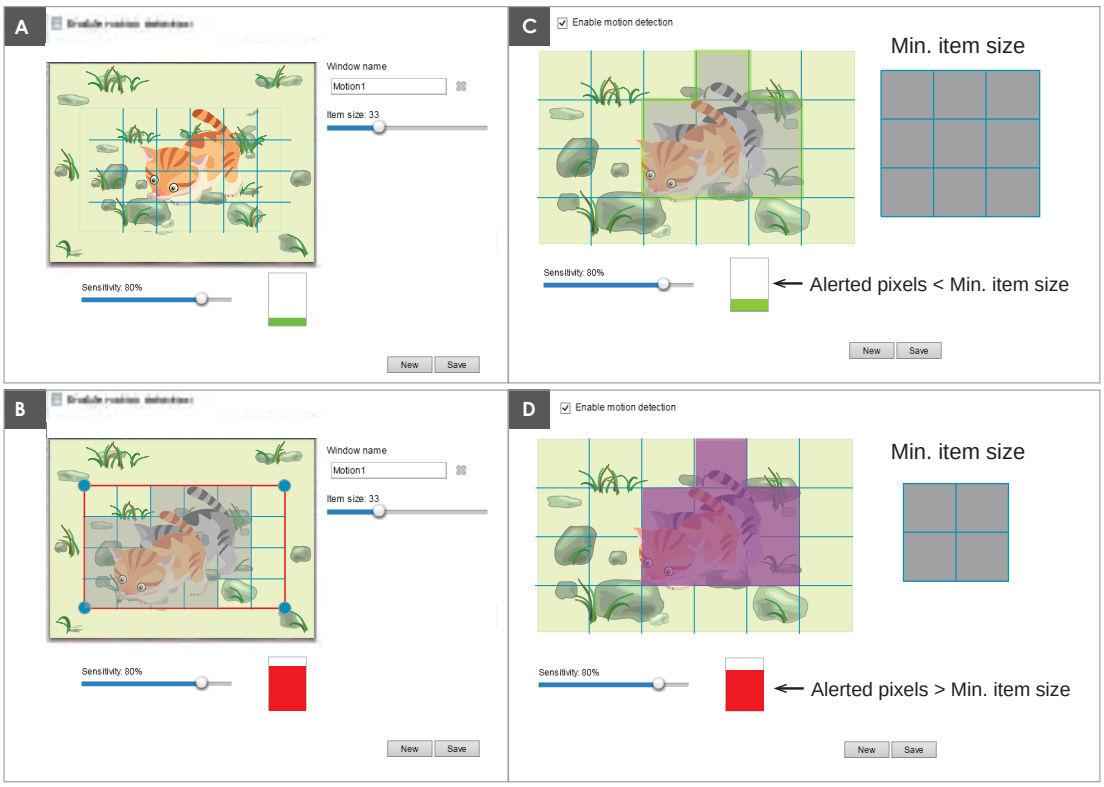


Please follow the steps beolw to set up a profile:
1. Create a new motion detection window.
2. Click the **Profile mode** tab.
3. Select the applicable Schedule mode. Please manually enter a time range.
4. Click **Save** to enable the settings and click **Close** to exit the page.

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.

NOTE:

► *How does motion detection work?*

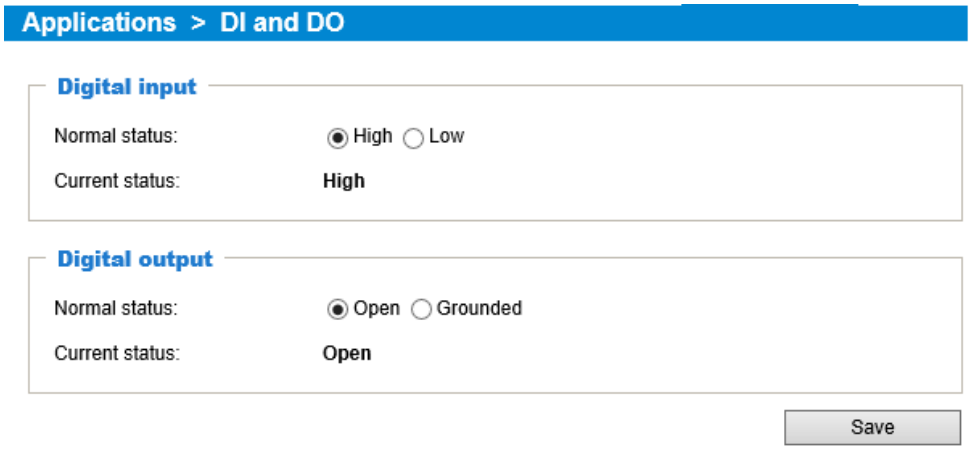


There are two motion detection parameters: Sensitivity and Min. Item Size. As illustrated above, frame A and frame B are two sequential images. Pixel differences between the two frames are detected and highlighted in gray in which the sensitivity setting will take effect. Sensitivity is a value that 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



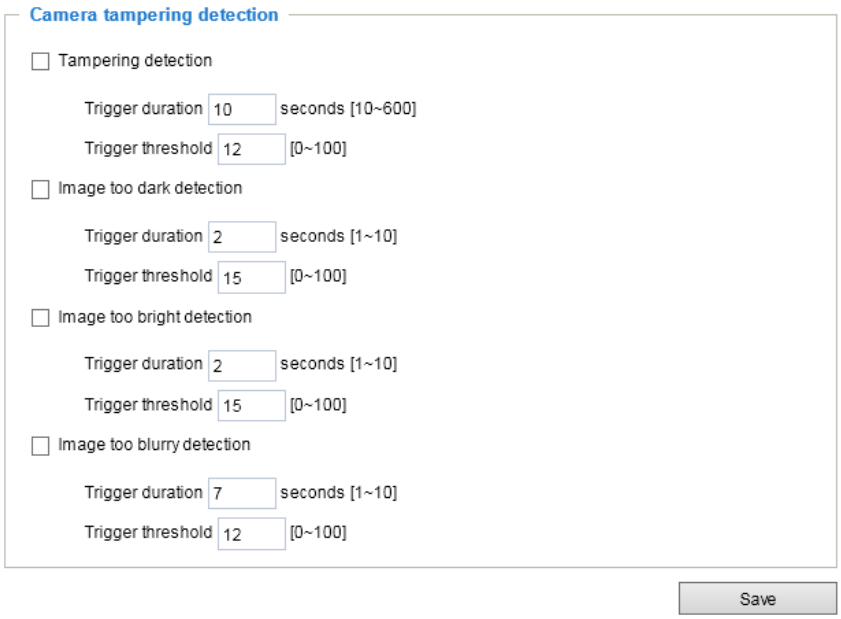
Digital input: Select High or Low as the Normal status for the digital input connection. Connect the digital input pin of the Network Camera to an external device to detect the current connection status.

Digital output: 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**.



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

1. 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.

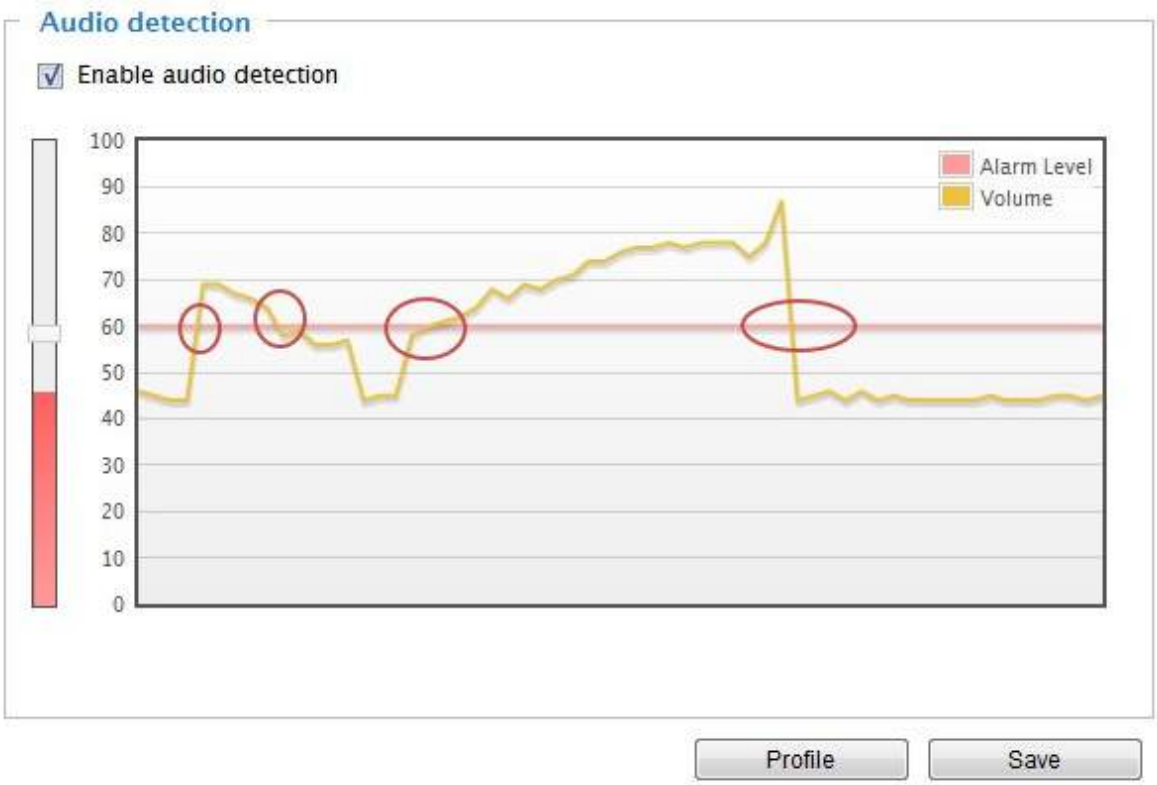
   The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold. Conditions such as image too dark, too bright, or too blurry (defocused) can also be configured as tampering conditions. The Trigger threshold 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.



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

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

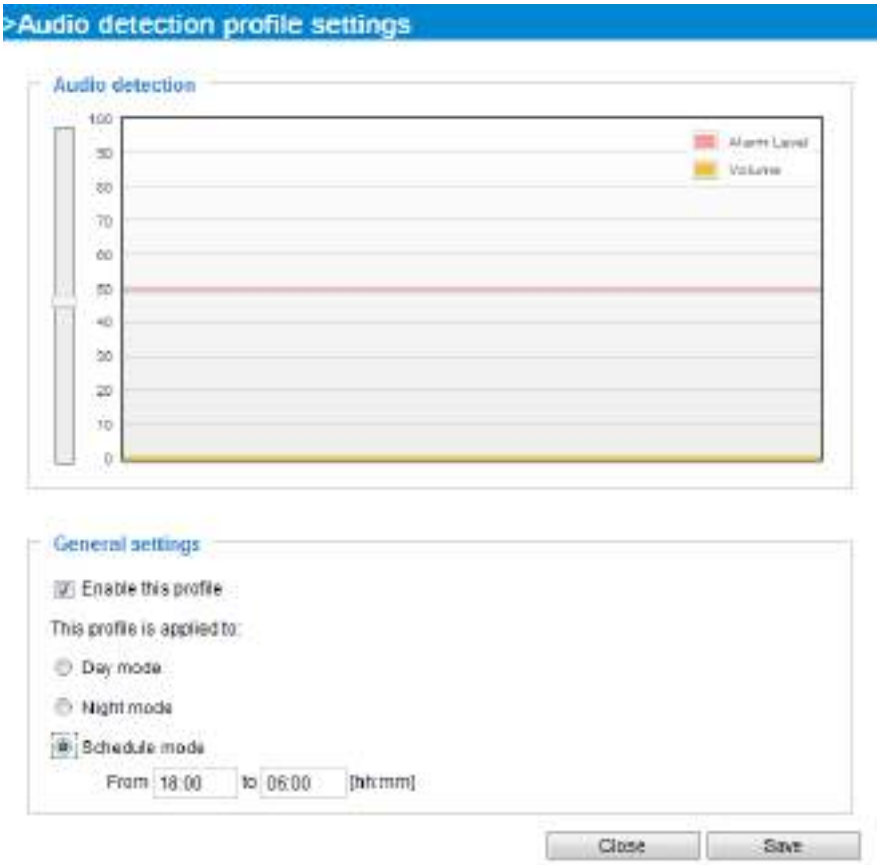
NOTE:

1. Note that the volume numbers (0~100) on the side of wave diagram does not represent decibel (dB). Sound intensity level has already been mapped to preset values. You can, however, use the real-world inputs at your installation site that are shown on the wave diagram to configure an alarm level.

2. To configure this feature, you must not mute the audio in **Configuration > Media > Audio**. *The default of the camera can be muted due to the lack of an internal microphone. An external microphone is provided by users.*

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

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



IMPORTANT:

- If the Alarm level and the received volume are set within a range of 20% on the wave diagram, frequent alarms will be triggered. It is recommended to set the Alarm level farther apart from the detected sound level.
- To configure and enable this feature, you **must not** configure video stream #1 into **Motion JPEG**. If an external microphone input is connected and recording of audio stream is preferred, audio stream is transmitted between camera and viewer/recording station **along with stream #1**.
- Refer to page 80 for Audio settings, and page 70 for video streaming settings.

Applications > Package management - a.k.a., VADP (VIVOTEK Application Development Platform)

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.

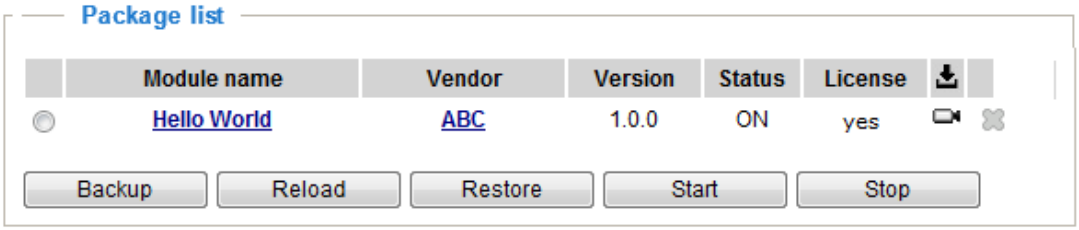
- Users can also run VIVOTEK's VADP packages as a means to access updated functionality instead of replacing the entire firmware.

- 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.

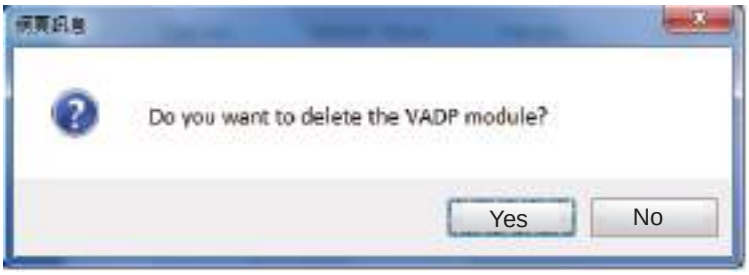
To utilize a software module, acquire the software package and click **Browse** and **Upload** buttons. The screen message for a successful upload is shown below:

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



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.

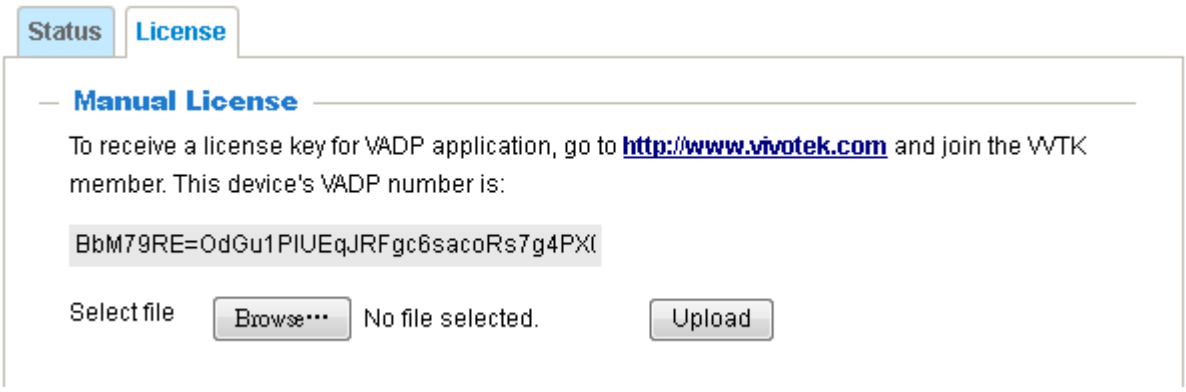
When prompted by a confirm message, Click **Yes** to proceed.



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.

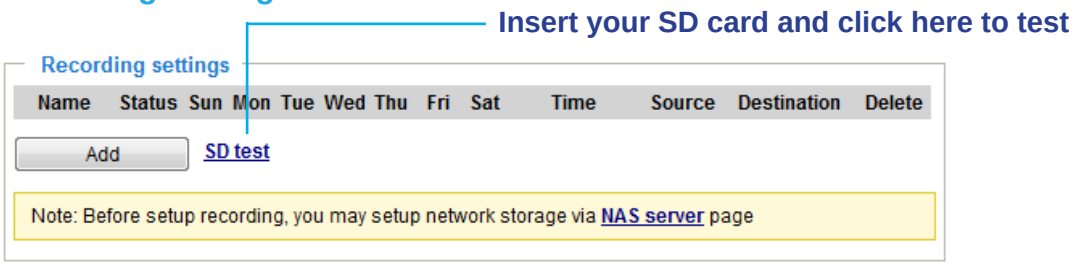
Follow the onscreen instruction on VIVOTEK's website for the registration procedure.



Recording > Recording settings

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

Recording Settings

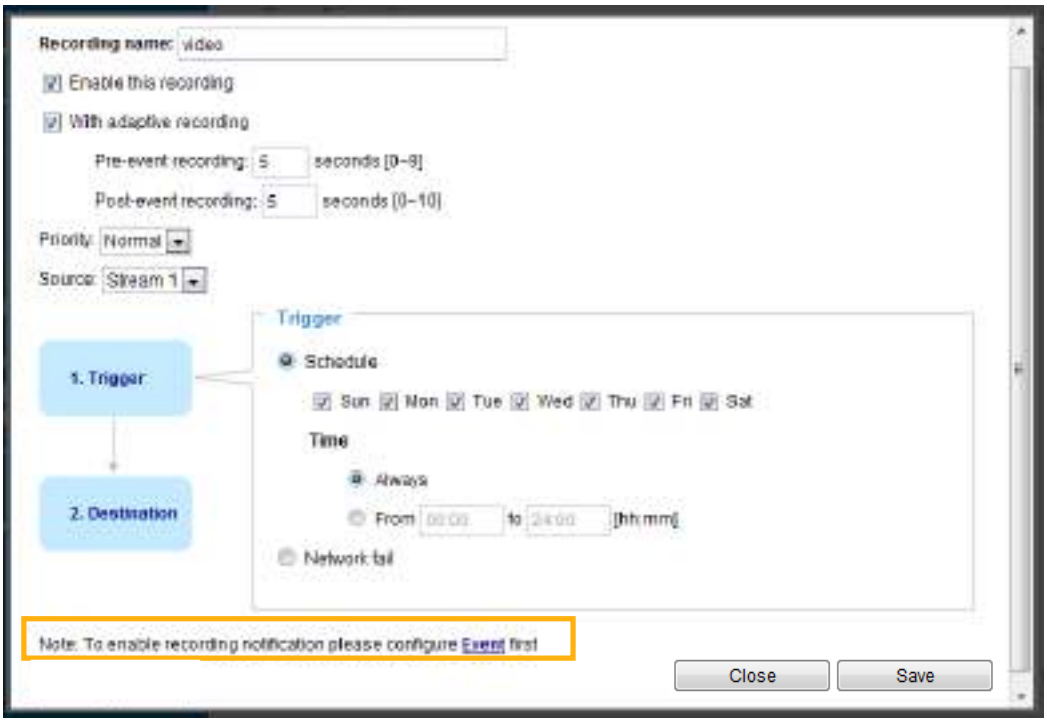


NOTE:

► *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.

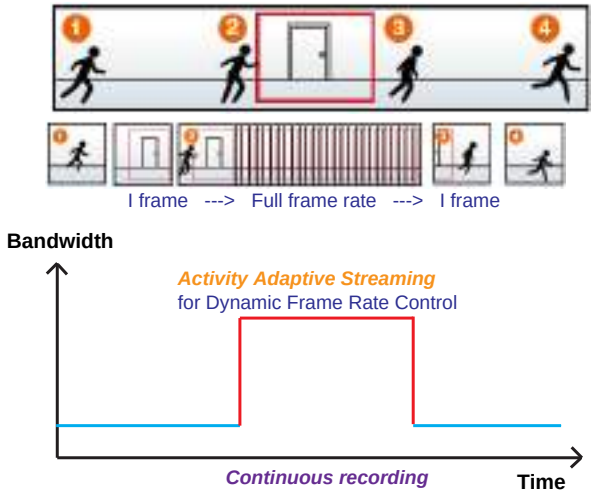


■ Recording name: Enter a name for the recording setting.

■ 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.



NOTE:

► *To enable adaptive recording, please make sure you've set up the trigger source such as Motion Detection, DI Device, or Manual Trigger.*

► *When there is no alarm trigger:*
- JPEG mode: record 1 frame per second.
- H.264 mode: record the I frame only.

► *When the I frame period is >1s on Video settings page, firmware will force decrease the I frame period to 1s when adaptive recording is enabled.*

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.

NOTE:

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

Please follow the steps below to set up the recording.

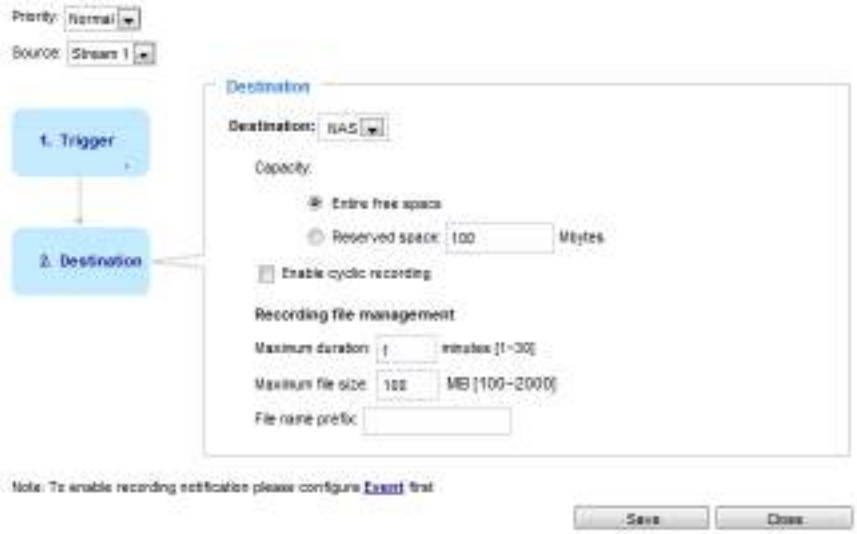
1. Trigger
Select a trigger source.

■ 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

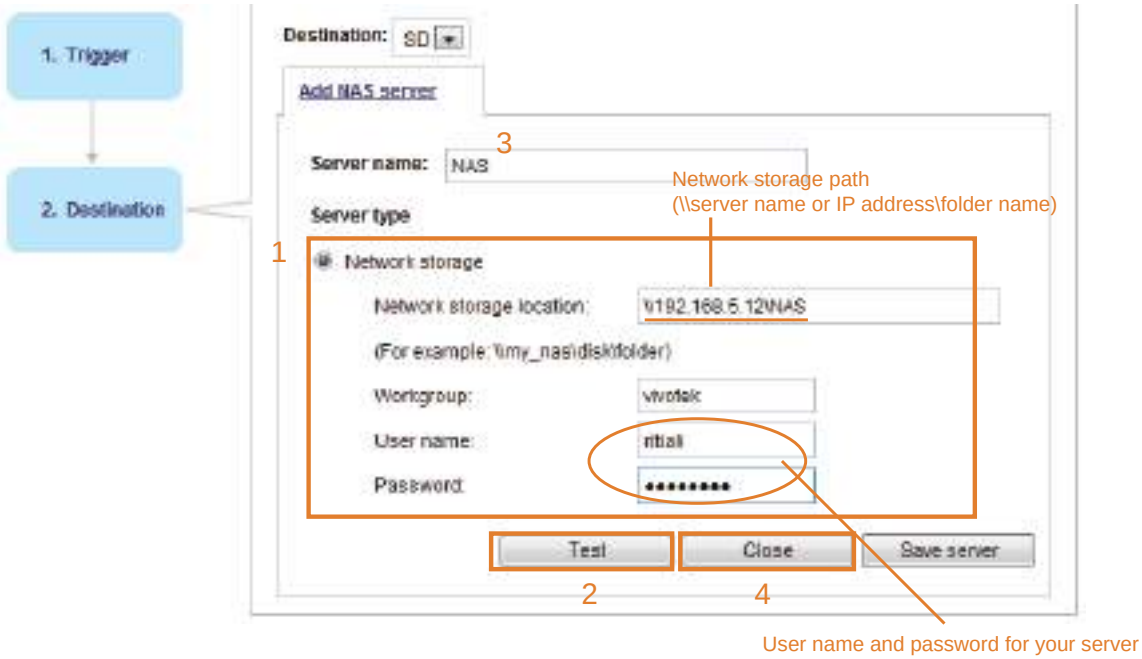
You can select the SD card or network storage (NAS) for the recorded video files. If you have not configured a NAS server, see details in the following.



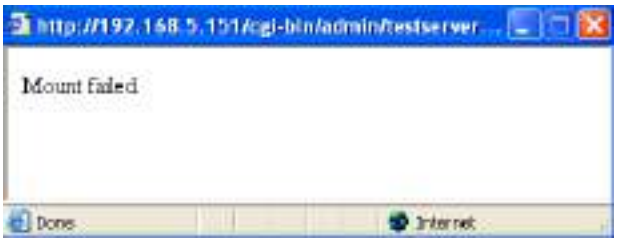
NAS server

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

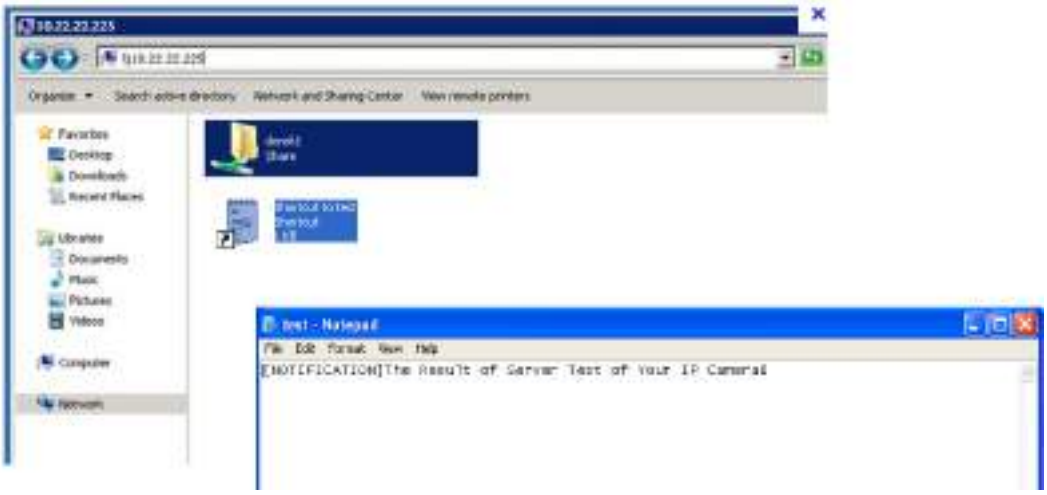
1. Fill in the information for your server.
   For example:



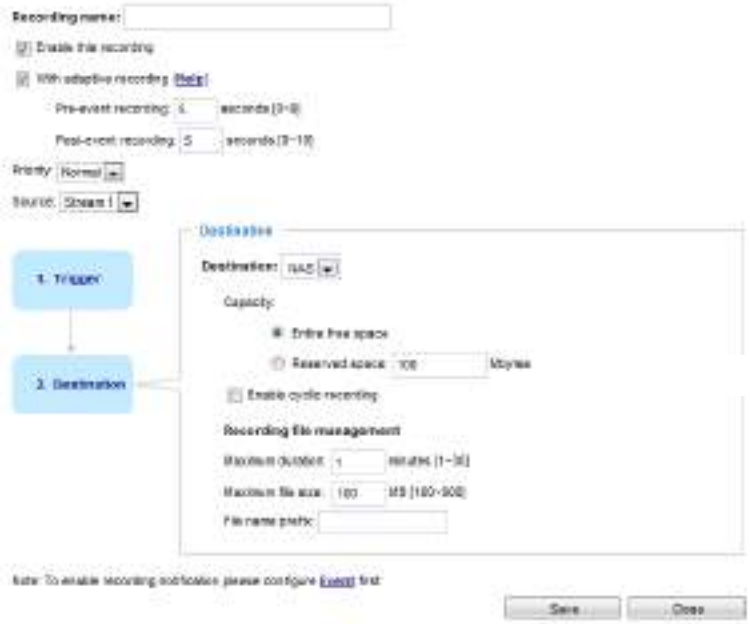
2. Click **Test** to check the setting. The result will be shown in the pop-up window.



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.



- 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.

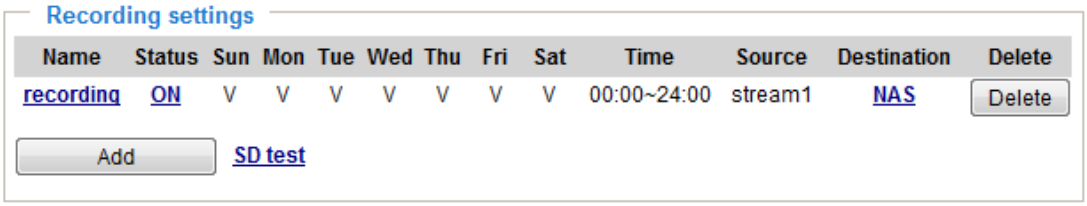
- Recording file management: You can manually assign the Maximum duration and the Maximum file size for each recording footage. You may need to stitch individual files together under some circumstances. You may also designate a file name prefix by filling in the responsive text field.

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

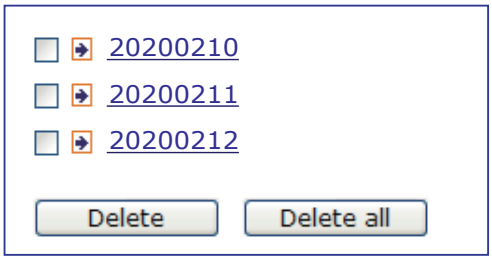
f you want to enable recording notification, please click ***Event*** to configure event triggering settings. Please refer to **Event > Event settings** on page 119 for more details.

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**.



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



Storage > SD card management

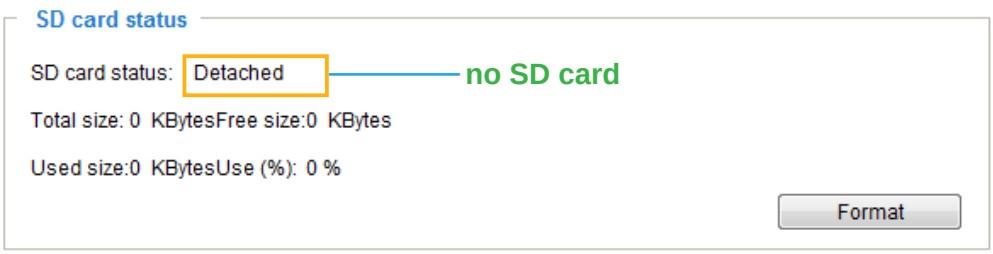
NOTE:

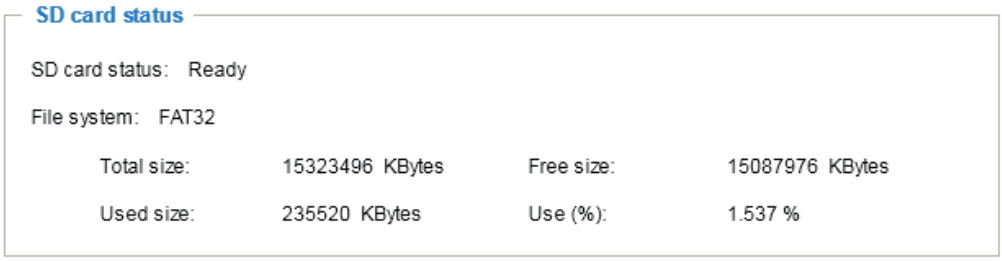
- It is recommended to turn OFF the recording activity before you remove an SD card from the camera.
- The lifespan of an SD card is limited. Regular replacement of the SD card can be necessary.
- Camera filesystem takes up several megabytes of memory space. The storage space cannot be used for recording.
- 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.

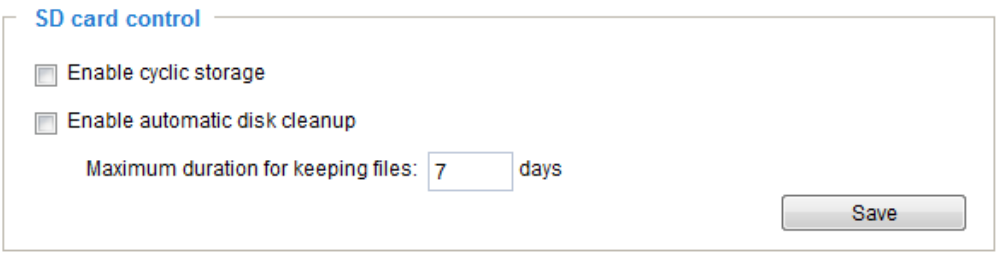




SD card format

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 control

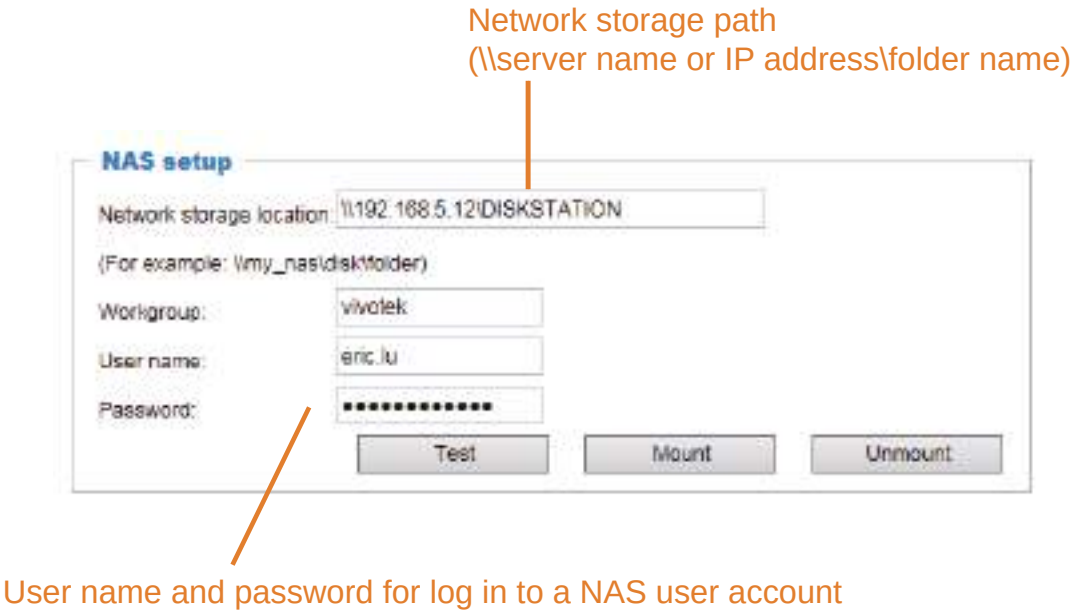


- Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.
- Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter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

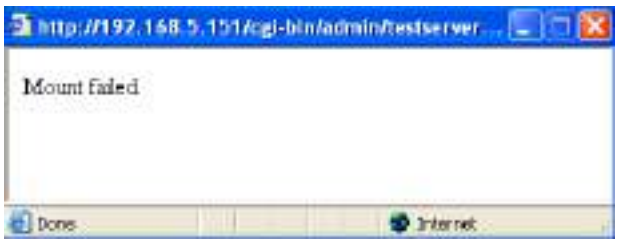
Click **Save** to enable your settings.

NAS management

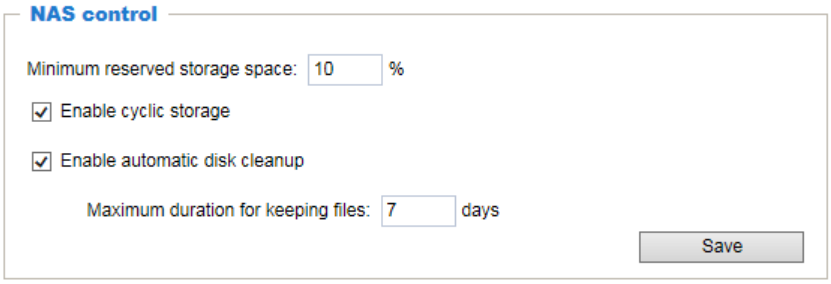
On the NAS setup page you can configure your NAS (Networked Storage) configuration, test, mount, or unmount the networked storage.



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



NAS control



- 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.

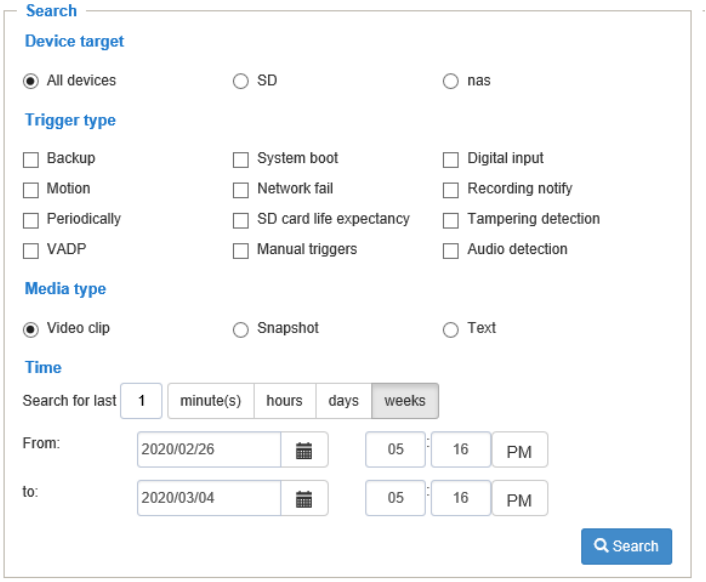
Click **Save** to enable your settings.

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.

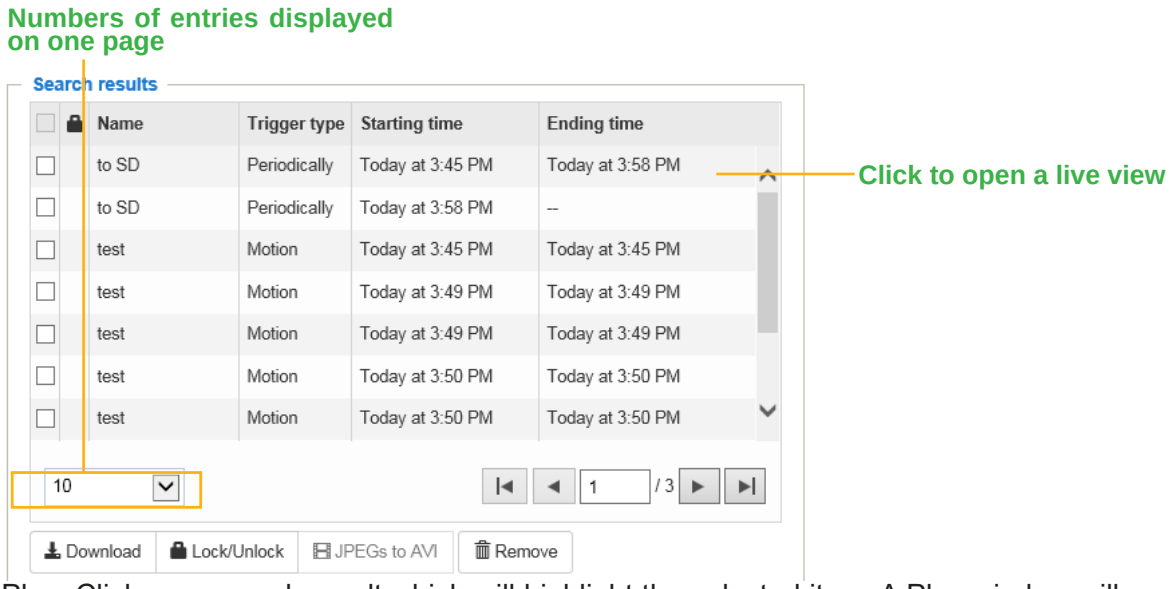


- File attributes: Select one or more items as your search criteria.
- Trigger time: Manually enter the time range you want to search for contents created at a specific point in time.

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.

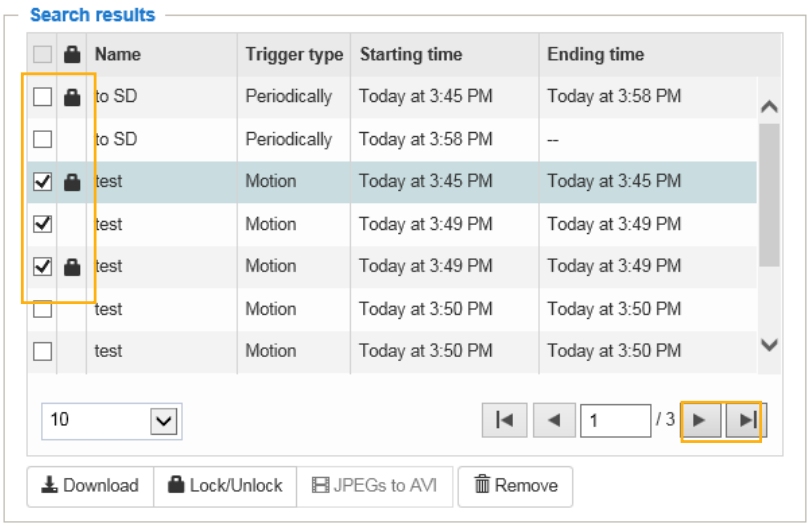


■ Play: Click on a search result which will highlight the selected item. A Play window will appear on top for immediate review of the selected file.
For example:

■ 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:



■ 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.

5. Get Server Parameter Values

Note: The access right depends on the URL directory.

Method: GET/POST

Syntax:

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

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

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

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

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

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

A successful control request returns parameter pairs as follows:

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>]

<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>	A full path like: "videoin_c0_s0_h264_resolution", "videoin_c0_s0_h264_maxframe", etc.
<value>	The assigned <value> to the <parameter>.
<return page>	Redirect to the page <return page>after the <parameter> is assigned. The <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>]	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>]	The same as string but displays'*' instead.
<integer>	Any single integer number in 32-bits. The range is -2147483648~2147483647.
<positive integer>	Any single positive integer number in 32-bits. The range is 1~ 4294967295.
<m> ~ <n>	Any number between 'm' and 'n'.
domain name[<n>]	A string limited to a domain name shorter than 'n' characters (eg. www.ibm.com).
email address [<n>]	A string limited to an email address shorter than 'n' characters (eg. joe@www.ibm.com).
<ip address>	A string limited to an IP address (eg. 192.168.1.1).
<mac address>	A string limited to contain a MAC address without hyphens or colons.
<boolean>	A boolean value of 1 or 0 represents [Yes or No], [True or False], [Enable or Disable].
<value1>, <value2>, <value3>, …	Enumeration. Only given values are valid.
blank	A blank string.
everything inside <>	A description
integer primary key	SQLite data type. A 32-bit signed integer. The value is assigned a unique integer by the server.
<text>	SQLite data type. The value is a text string, stored using the database encoding (UTF-8, UTF-16BE or UTF-16-LE).
<coordinate>	x, y coordinate (eg. 0,0)
<window size>	window width and height (eg. 800x600)
<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>	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>	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.

7.1 System

Group: **system**

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
	<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 (get/set)	DESCRIPTION
			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>	6/6	Enable automaticdaylight saving time in time zone.
daylight_dstactualmode	<positive integer>	6/7	Check if current time is under daylight saving time. (Used internally)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
daylight_auto_begintime	string[19]	6/7	Display the current daylight saving start 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, 3600, 86400, 604800, 2592000	6/6	0 to Disable automatic time adjustment, otherwise, it indicates the seconds between NTP automatic update intervals.
restore	0, <positive integer>	7/6	Restore the system parameters to default values after <value> seconds.
reset	0, <positive integer>	7/6	Restart the server after <value> seconds if <value> is non-negative.
restoreexceptnet	0, <positive integer>	7/6	Restore the system parameters to default values except (ipaddress, subnet, router, dns1, dns2, pppoe). This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptdst	0, <positive integer>	7/6	Restore the system parameters to default values except all daylight saving time settings. This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to default values except for a union of combined results.
restoreexceptlang	0,	7/6	Restore the system parameters to default

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
	<positive integer>		values except the custom language file the user has uploaded. This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptvadp	0, <positive integer>	7/6	Restore the system parameters to default values except the vadp parameters and VADP modules that stored in the system. This command can cooperate with other “restoreexceptXYZ” commands. When cooperating with others, the system parameters will be restored to the default value except for a union of the combined results.
restoreexceptfocusvalue	0, <positive integer>	7/6	Restore the system parameters to default values except zoom and focus value. 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)>_remotefocus" != 0.
restoreexceptlen	0, <positive integer>	7/6	Restore the system parameters to default values except lens profile. 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 (get/set)	DESCRIPTION
			* Only available when "capability_image_c<0~(n-1)>_lensconfiguration_support" != 0.

7.1.1 System.Info

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
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>	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>
language_count	<positive integer>	0/7	Number of webpage languages available on the server.
language_i<0~(count-1)>	string[16] language_i0 : English language_i1 : Deutsch language_i2 : Español language_i3 : Français language_i4 : Italiano language_i5 : 日本語 language_i6 : Português	0/7	Available language lists.

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

7.2 Status

Group: **status**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
di_i<0~(capability_ndi-1)> <product dependent>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered (capability_ndi > 0)
do_i<0~(capability_ndo-1)> <product dependent>	<boolean>	1/7	0 => Inactive, normal 1 => Active, triggered (capability_ndo > 0)
onlinenum_rtsp	0,<positive integer>	6/7	Current number of RTSP connections.
onlinenum_httppush	0,<positive integer>	6/7	Current number of HTTP push server connections.
onlinenum_sip	0,<positive integer>	6/7	Current number of SIP connections.
eth_i0	<string>	1/7	Get network information from mii-tool.
vi_i<0~(capability_nvi-1)> <product dependent>	<boolean>	1/7	Virtual input 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 (get/set)	DESCRIPTION
signal_detect	<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 (get/set)	DESCRIPTION
normalstate	high, low	1/1	Indicates open circuit or closed circuit (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 (get/set)	DESCRIPTION
normalstate	open, grounded	1/1	Indicate open circuit or closed circuit (inactive status)

7.5 Security

1. Group: **security**

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

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
privilege_camctrl	view, operator, admin	1/6	Indicate which privileges and above 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, operator, admin	6/7	Root privilege
user_i<1~20>_ privilege	view, operator, admin	6/6	User privilege

7.6 Network

Group: **network**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
preprocess	<positive integer>	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 (get/set)	DESCRIPTION
			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, pppoe	6/6	Network connection type.
resetip	<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>	6/6	IP address of server.
subnet	<ip address>	6/6	Subnet mask.
router	<ip address>	6/6	Default gateway.
dns1	<ip address>	6/6	Primary DNS server.
dns2	<ip address>	6/6	Secondary DNS server.
wins1	<ip address>	6/6	Primary WINS server.
wins2	<ip address>	6/6	Secondary WINS server.

7.6.1 802.1x

Subgroup of **network: ieee8021x** (capability_protocol_ieee8021x > 0)

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

7.6.2 QOS

Subgroup of **network: qos_cos** (capability_protocol_qos_cos > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
enable	<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 <product dependent>	0~7	6/6	Audio channel for CoS (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 (get/set)	DESCRIPTION
enable	<boolean>	6/6	Enable/disable DSCP
video	0~63	6/6	Video channel for DSCP

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

7.6.4 FTP

Subgroup of **network**: **ftp**

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

7.6.5 HTTP

Subgroup of **network**: **http**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	80, 1025 ~ 65535	1/6	HTTP port.
alternateport	1025~65535	6/6	Alternate HTTP port.
authmode	basic, digest	1/6	HTTP authentication mode.
s<0~(capability_nmediastream-1)>_accessname <product dependent> <Not recommended to use this>	string[32]	1/6	Http server push access name for stream N, N= 1~ capability_nmediastream. (capability_protocol_spush_mjpeg =1 and capability_nmediastream > 0) The value are shown as video1s1.mjpg = c0_s0_accessname, (channel1stream1) video1s2.mjpg = c0_s1_accessname, (channel1stream2) video1s3.mjpg = c0_s2_accessname, (channel1stream3) video1s4.mjpg = c0_s3_accessname, (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>	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 (get/set)	DESCRIPTION
s<0~(capability_nmedia stream-1)>_accessname <product dependent>	string[32]	1/6	Http server push access name for channel N and stream M, N= 1~ capability_nvideoin, M= 1~ capability_nmediastream. (capability_protocol_spush_mjpeg =1 and capability_nmediastream > 0) The value are shown as video1s1.mjpg = c0_s0_accessname, (channel1stream1) video1s2.mjpg = c0_s1_accessname, (channel1stream2) video2s1.mjpg = c1_s0_accessname, (channel2stream1) video2s2.mjpg = c1_s1_accessname, (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 (get/set)	DESCRIPTION
port	443, 1025 ~ 65535	1/6	HTTPS port.

7.6.8 RTSP

Subgroup of **network**: **rtsp** (capability_protocol_rtsp > 0)

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
port	554, 1025 ~ 65535	1/6	RTSP port. (capability_protocol_rtsp=1)
anonymousviewing	<boolean>	1/6	Enable anoymous streaming viewing.
authmode	disable, basic, digest	1/6	RTSP authentication mode. (capability_protocol_rtsp=1)
s<0~(capability_nmediastream*capability_nvideoin)-1)>_accessname <product dependent>	string[32]	1/6	RTSP access name for channel/stream N, N= 1~ capability_nmediastream. (capability_protocol_spush_mjpeg =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 (get/set)	DESCRIPTION
alwaysmulticast	<boolean>	4/4	Enable always multicast.
ipaddress	<ip address>	4/4	Multicast video IP address. * We replace

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
			"network_rtsp_s<0~(n-1)>_multicast_ipaddress" with " network_rtsp_s<0~(n-1)>_multicast_videoipaddress ". * Reserved for compatibility, and suggest don't use this since [httpversion] > 0304a
videoipaddress	<ip address>	4/4	Multicast video IP address. * We support this parameter when the version number (httpversion) is equal or greater than 0304a.
audioipaddress <product dependent>	<ip address>	4/4	Multicast audio IP address. * We support this parameter when the version number (httpversion) is equal or greater than 0304a. * Only available when capability_naudioin > 0
metadataipaddress	<ip address>	4/4	Multicast metadata IP address. * We support this parameter when the version number (httpversion) is equal or greater than 0304a.
videoport	1025 ~ 65535	4/4	Multicast video port.
audioport <product dependent>	1025 ~ 65535	4/4	Multicast audio port. * Only available when capability_naudioin > 0
metadataport	1026~65534	4/4	Multicast metadata port.
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 (get/set)	DESCRIPTION
port	1025 ~ 65535	1/6	SIP port.

7.6.11 RTP Port

Subgroup of **network**: **rtp**

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

7.7 IP Filter

Group: **ipfilter**

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

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

7.8 Video Input

Group: **videoin**

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
cmosfreq	50, 60	4/4	CMOS frequency. * Only available when capability_videoin_type is 2.
whitebalance <product dependent>	auto, panorama, manual, rbgain, widerange, outdoor, indoor, sodiumauto, etc (Available values are listed in "capability_image_c<0~(n-1)>_wbmode")	4/4	Modes of white balance. **"auto"**: Auto white balance **"panorama"**: indicates that camera would try to balance the white balance effect of every sensor. **"rbgain"**: Use rgain and bgain to set white balance manually. **"manual"**: 2 cases: a. if "rbgain" is not supported, this means keep current white balance status. b. if "rbgain" is supported, "rgain" and "bgain" are updated to the 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.

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
			"sodiumauto": sodium vapor lamps. * Only available when "capability_image_c<0~(n-1)>_wbmode" !="-"
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)>_exposure_mode" !=0
irismode	fixed, indoor, outdoor <product independent>	4/4	Control DC-Iris mode. **"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. * Only available when "capability_image_c<0~(n-1)>_iristype"=dciris
enableblc	<boolean>	4/4	Enable backlight compensation.

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
<Not support anymore>			* 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.
color	0, 1	4/4	0 =>monochrome 1 => color * Only available when " capability_videoin_c<0~(n-1)>_color_ support" is 1.
flip	<boolean>	4/4	Flip the image.
mirror	<boolean>	4/4	Mirror the image.
rotate	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
ptzstatus <Not support anymore>	0,<positive integer>	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 =>**Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)(SD/PZ/IZ series only)
text	string[64]	1/4	Enclose caption.

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video.
minexposure <product dependent>	<1~32000>, <5~32000>, <1~8000>, <5~8000>, etc. * Available value is listed in "capability_image_c<0~(n-1)>_exposure_minrange"	4/4	Minimum exposure time 1~32000 => 1s ~ 1/32000s 5~32000 => 1/5s ~ 1/32000s 1~8000 => 1s ~ 1/8000s 5~8000 => 1/5s ~ 1/8000s etc. * Only available when "capability_image_c<0~(n-1)>_exposure_minrange" != "-" * Only valid when "piris_mode"=manual or "irismode"=fixed * Only available when "capability_image_c<0~(n-1)>_exposure_rangetype" is "twovalues".
maxexposure <product dependent>	<1~32000>, <5~32000>, <1~8000>, <5~8000>, etc. * Available value is listed in "capability_image_c<0~(n-1)>_exposure_maxrange"	4/4	Maximum exposure time 1~32000 => 1s ~ 1/32000s 5~32000 => 1/5s ~ 1/32000s 1~8000 => 1s ~ 1/8000s 5~8000 => 1/5s ~ 1/8000s etc. * This parameter may also restrict image frame rate from sensor due to 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)>_exposure_maxrange" != "-" * Only valid when "piris_mode"=manual or "irismode"=fixed * Only available when

NAME	VALUE	SECURITY (get/set)	DESCRIPTION
			"capability_image_c<0~(n-1)>_exposure_rangetype" is "twovalues".
enablepreview	<boolean>	1/4	Usage for UI of exposure settings. Preview settings of video profile. * Only available when "capability_image_c<0~(n-1)>_exposure_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(get/set)	DESCRIPTION
cmosfreq	50, 60	4/4	CMOS frequency. * Only available when " capability_videoin_type " is 2
mode	0 ~ "capability_videoin_c<0~(n-1)>_nmode"-1	4/4	Indicate the video mode on use.
whitebalance <product dependent>	auto, panorama, manual, rbgain, widerange, outdoor, indoor, sodiumauto, etc (Available values are listed in "capability_image_c<0~(n-1)>_wbmode")	4/4	Modes of white balance. **"auto"**: Auto white balance **"panorama"**: indicates that camera would try to balance the white balance effect of every sensor. **"rbgain"**: Use rgain and bgain to set white balance manually. **"manual"**: 2 cases: a. if "rbgain" is not supported, this means keep current white balance status. b. if "rbgain" is supported, "rgain" and "bgain" are updated to the 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(get/set)	DESCRIPTION
			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)>_wbmode". * 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)>_wbmode". * 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(get/set)	DESCRIPTION
			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)>_exposure_mode" !=0
exposuremode <product dependent>	auto, shutterpriority, irispriority, qualitypriority, manual, etc (Available options are list in "capability_image_c<0~(n-1)>_exposure_modetype")	4/4	Select exposure mode. **"auto"**: Automatically adjust the Iris, Gain and Shutter Speed to fit the exposure level. **"shutterpriority"**: Manually adjust with variable Shutter Speed, and keep adjusting Iris, Gain automatically. **"irispriority"**: Manually adjust with variable Iris, and keep adjusting Gain and Shutter speed automatically. **"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)>_exposure_mode" !=0
irismode	fixed, indoor, outdoor <product dependent>	4/4	Control DC-Iris mode. **"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(get/set)	DESCRIPTION
			* Only available when "capability_image_c<0~(n-1)>_iristype"=dciris
piris_mode <product dependent>	manual, indoor, outdoor,-	1/4	Control P-Iris mode. **"outdoor"**: Auto-setting P-Iris to get 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 <product dependent>	1~100	1/4	Manual set P-Iris. 1: Open <-> 100: Close * 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 <Not support anymore>	<boolean>	4/4	Enable backlight compensation * 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.
maxgain	0~100	4/4	Maximum gain value.

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
			0: Low <-> 100: High * Only available when "capability_image_c<0~(n-1)>_agc_maxgain" != "-" * Only valid when "piris_mode"=manual or "irismode"=fixed * Normalized range. * Only available when "capability_image_c<0~(n-1)>_exposure_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_mingain" != "-" * Only valid when "piris_mode"=manual or "irismode"=fixed * Normalized range. * Only available when "capability_image_c<0~(n-1)>_exposure_rangetype" is "twovalues".
gainvalue	0~100	4/4	Gain value. 0: Low <-> 100: High * Only available when "capability_image_c<0~(n-1)>_agc_maxgain" != "-" and "capability_image_c<0~(n-1)>_exposure_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(get/set)	DESCRIPTION
			* Only available when " capability_videoin_c<0~(n-1)>_color_support" is 1.
flip	<boolean>	4/4	Flip the image.
mirror	<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)>_rotation=1)
ptzstatus <Not support anymore>	0,<positive integer>	1/7	A 32-bit integer, each bit can be set separately as follows: Bit 0 => Support camera control function; 0(not support), 1(support) Bit 1 =>**Built-in** or **external** camera; 0 (external), 1(built-in) Bit 2 => Support **pan** operation; 0(not support), 1(support) Bit 3 => Support **tilt** operation; 0(not support), 1(support) Bit 4 => Support **zoom** operation; 0(not support), 1(support) Bit 5 => Support **focus** operation; 0(not support), 1(support)(SD/PZ/IZ series only)
text	string[64]	1/4	Enclose caption.
imprinttimestamp	<boolean>	4/4	Overlay time stamp on video.
textonvideo_position	top, bottom	4/4	Text on video string position
textonvideo_size	20~40	4/4	Text on video font size
textonvideo_fontpath	/usr/share/font/Default.ttf, /mnt/flash2/upload.ttf	4/4	Choose camera default font file (/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(get/set)	DESCRIPTION
ploadfilename	name uploaded by user		
minexposure <product dependent>	<1~32000>, <5~32000>, <1~8000>, <5~8000>, etc. * Available value is listed in "capability_image_c<0~(n-1)>_exposure_minrange"	4/4	Minimum exposure time 1~32000 => 1s ~ 1/32000s 5~32000 => 1/5s ~ 1/32000s 1~8000 => 1s ~ 1/8000s 5~8000 => 1/5s ~ 1/8000s etc. * Only available when "capability_image_c<0~(n-1)>_exposure_minrange" != "-" * Only valid when "piris_mode"=manual or "irismode"=fixed * Only available when "capability_image_c<0~(n-1)>_exposure_rangetype" is "twovalues".
maxexposure <product dependent>	<1~32000>, <5~32000>, <1~8000>, <5~8000>, etc. * Available value is listed in "capability_image_c<0~(n-1)>_exposure_maxrange"	4/4	Maximum exposure time 1~32000 => 1s ~ 1/32000s 5~32000 => 1/5s ~ 1/32000s 1~8000 => 1s ~ 1/8000s 5~8000 => 1/5s ~ 1/8000s etc. * This parameter may also restrict image frame rate from sensor due to 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)>_exposure_maxrange" != "-" * Only valid when "piris_mode"=manual or "irismode"=fixed * Only available when

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

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
			* We support this parameter when the version number (httpversion) is equal or greater than 0311a.
crop_position	<coordinate> (x,y)	1/7	Crop left-top corner coordinate.
crop_size	<window size> (WxH)	1/7	Crop width and height. (width must be 16x or 32x and height must be 8x)
zoomratiodisplay	<boolean>	1/4	Indicates multiple of zoom in is “on-screen display” or not. * We support this parameter when the version number (httpversion) is equal or greater than 0302a.
bracketing_level	1~100	4/4	● The total available lists (capability_image_c<0~(n-1)>_exposure_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)>_exposure_bracketing_mode"=1. * We support this parameter when the version number (httpversion) is equal or greater than 0310a.
s<0~(m-1)>_enableeptz	<boolean>	4/4	Indicate whether stream supprts eptz or not
s<0~(m-1)>_codectype	Listed at "capability_videoin_codec" Possible values are: mjpeg, h264,h265 <product dependent>	1/4	Codec type for this stream
s<0~(m-1)>_re	Available options are list in	1/4	Video resolution in pixels.

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
solution	"capability_videoin_c<0~(n-1)>_resolution". Besides, available options is referred to "capability_videoin_c<0~(n-1)>_maxresolution" and "capability_videoin_c<0~(n-1)>_minresolution"		
s<0~(m-1)>_smartfps_enable	<boolean>	4/4	Enable "Smart fps" function. * Only available when "capability_videoin_c<0~(n-1)>_smartfps_support" is 1. * We support this parameter when the version number (httpversion) is equal or greater than 0309a.
s<0~(m-1)>_h264_dintraperiod_enable	<boolean>	4/4	Enable "Dynamic intra frame period". * Only available when "capability_videoin_c<0~(n-1)>_dintraperiod_support" is 1. * We support this parameter when the version number (httpversion) is equal or greater than 0301c.
s<0~(m-1)>_h264_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	The time interval between two I-frames (Intra coded picture). The unit is millisecond (ms).
s<0~(m-1)>_h264_ratecontrolmode	cbr, vbr	4/4	**cbr**: Constant bit rate mode. **vbr**: Fixed quality mode, all frames are encoded in the same quality.
s<0~(m-1)>_h264_quant	1~5, 99, 100	4/4	Set the pre-defined quality level: 1: Medium 2: Standard 3: Good 4: Detailed 5: Excellent 100: Use the quality level in

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
			"qpercent" 99: Use the quality level in "qvalue" * Only valid when "h264_ratecontrolmode"= vbr.
s<0~(m-1)>_h264_qvalue	0~51	4/4	Manual video quality level input. The 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)>_h264_qpercent	1~100	4/4	Select customized quality in a normalized full range. 1: Worst quality 100: Best quality * Only valid when "h264_ratecontrolmode"= vbr and "quant"= 100.
s<0~(m-1)>_h264_maxvbrbitrate	20000~"capability_videoin_c<0~(n-1)>_h264_maxbitrate"	4/4	The maximum allowed bit rate in fixed quality mode. 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)>_h264_cbr_quant	1~5, 100	4/4	Set the pre-defined quality level: 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(get/set)	DESCRIPTION
			"2.0"
s<0~(m-1)>_h264_cbr_qpercent	1~100	4/4	Select customized quality in a normalized full range. 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)>_h264_bitrate	20000~"capability_videoin_c<0~(n-1)>_h264_maxbitrate"	4/4	The target bit rate in constant bit rate mode. * Only valid when "h264_ratecontrolmode"= cbr
s<0~(m-1)>_h264_prioritypolicy	framerate,imagequality	4/4	Set prioritypolicy * Only valid when "h264_ratecontrolmode"= cbr
s<0~(m-1)>_h264_maxframe	1~"capability_videoin_c<0~(n-1)>_h264_maxframerate"	1/4	The maximum frame rates of a H264 stream at different resolutions("capability_videoin_c<0~(n-1)>_resolution") are recorded in "capability_videoin_c<0~(n-1)>_h264_maxframerate"
s<0~(m-1)>_h264_profile	0~2	1/4	Indicate H264 profiles 0: baseline 1: main profile 2: high profile
s<0~(m-1)>_h264_smartq_enable	<boolean>	4/4	Enable "Smart Q" function. * Only available when "capability_videoin_c<0~(n-1)>_smartq_support" is 1. * We support this parameter when the version number (httpversion) is equal or greater than 0309a.
s<0~(m-1)>_h2	<boolean>	4/4	Enable "Dynamic intra frame period".

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
65_dintraperiod_enable			* Only available when "capability_videoin_c<0~(n-1)>_dintraperiod_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)>_h265_intraperiod	250, 500, 1000, 2000, 3000, 4000	4/4	The time interval between two I-frames (Intra coded picture). The unit is millisecond (ms). * Only available when h265 is listed in "capability_videoin_codec".
s<0~(m-1)>_h265_ratecontrolmode	cbr, vbr	4/4	**cbr**: Constant bit rate mode. **vbr**: Fixed quality mode, all frames are encoded in the same quality. * Only available when h265 is listed in "capability_videoin_codec".
s<0~(m-1)>_h265_quant	1~5, 99, 100	4/4	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" * Only available when h265 is listed in "capability_videoin_codec" and "h265_ratecontrolmode"= vbr.
s<0~(m-1)>_h265_qvalue	0~51	4/4	Manual video quality level input. The 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(get/set)	DESCRIPTION
			s<0~(m-1)>_h265_quant = 99.
s<0~(m-1)>_h265_qpercent	1~100	4/4	Select customized quality in a 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)>_h265_maxvbrbitrate	20000~"capability_videoin_c<0~(n-1)>_h265_maxbitrate"	4/4	The maximum allowed bit rate in fixed quality mode. 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)>_h265_cbr_quant	1~5, 100	4/4	Set the pre-defined quality level: 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)>_h265_cbr_qpercent	1~100	4/4	Select customized quality in a normalized full range. 1: Worst quality

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
			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)>_h265_bitrate	20000~"capability_videoin_c<0~(n-1)>_h265_maxbitrate"	4/4	The target bit rate in constant bit rate mode. * Only available when h265 is listed in "capability_videoin_codec". * Only valid when "h265_ratecontrolmode"= cbr
s<0~(m-1)>_h265_prioritypolicy	framerate,imagequality	4/4	Set prioritypolicy * Only available when h265 is listed in "capability_videoin_codec". * Only valid when "h265_ratecontrolmode"= cbr
s<0~(m-1)>_h265_maxframe	1~"capability_videoin_c<0~(n-1)>_h265_maxframerate"	1/4	The maximum frame rates of a H265 stream at different 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)>_h265_profile	Available values are listed in " capability_videoin_c<0~(n-1)>_h265_profile"	1/4	Indicate H265 profiles * Only available when h265 is listed in "capability_videoin_codec".
s<0~(m-1)>_h265_smartq_enable	<boolean>	4/4	Enable "Smart Q" function. * Only available when h265 is listed in "capability_videoin_codec". * Only available when

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
			"capability_videoin_c<0~(n-1)>_smartq_support" is 1. * We support this parameter when the version number (httpversion) is equal or greater than 0309a.
s<0~(m-1)>_mjpeg_ratecontrolmode	cbr, vbr	4/4	**cbr**: Constant bit rate mode. **vbr**: Fixed quality mode, all frames are encoded in the same quality.
s<0~(m-1)>_mjpeg_quant	1~5, 99, 100	4/4	* Only valid when "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)>_mjpeg_qvalue	10~200 (Only valid when "capability_api_httpversion" format is XXXXX_1 or XXXXX_3 or XXXXX_4 ex: 0301a_1 or 0301a_3 or 0301a_4) or 1~99 (Only valid when "capability_api_httpversion" format is XXXXX_2, ex: 0301a_2) <product dependent>	4/4	Manual video quality level input. The Q value which is used by encoded library directly. * Only valid when "mjpeg_ratecontrolmode"= vbr and s<0~(m-1)>_mjpeg_quant = 99
s<0~(m-1)>_mjpeg_qpercent	1~100	4/4	Select customized quality in a normalized full range. 1: Worst quality

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
			100: Best quality * Only valid when "mjpeg_ratecontrolmode"= vbr and s<0~(m-1)>_mjpeg_quant = 100.
s<0~(m-1)>_mjpeg_maxvbrbitrate	20000~"capability_videoin_c<0~(n-1)>_mjpeg_maxbitrate"	4/4	The maximum allowed bit rate in fixed quality mode. 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)>_mjpeg_cbr_quant	1~5, 100	4/4	Set the pre-defined quality level: 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)>_mjpeg_cbr_qpercent	1~100	4/4	Select customized quality in a normalized full range. 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)>_mjpeg_bitrate	20000~"capability_videoin_c<0~(n-1)>_mjpeg_maxbi	4/4	The target bit rate in constant bit rate mode.

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
	trate"		* Only valid when "mjpeg_ratecontrolmode"= cbr
s<0~(m-1)>_mjpeg_prioritypolicy	framerate,imagequality	4/4	Set prioritypolicy * Only valid when "mjpeg_ratecontrolmode"= cbr
s<0~(m-1)>_mjpeg_maxframe	1~"capability_videoin_c<0~(n-1)>_mjpeg_maxframerate"	1/4	The maximum frame rates of a mjpeg stream at different resolutions("capability_videoin_c<0~(n-1)>_resolution") are recorded in "capability_videoin_c<0~(n-1)>_mjpeg_maxframerate"
s<0~(m-1)>_ratiocorrect	<boolean>	1/4	Change resolution to fit 4:3 ratio. For PAL: D1/4CIF(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 <product dependent>	<boolean>	4/4	Enable WDR pro * Only available when "capability_image_c<0~(n-1)>_wdrpro_mode" > 0
wdrpro_strength <product dependent>	1~100	4/4	The strength of WDR Pro. The bigger value means the stronger strength of WDR Pro. * Only available when "capability_image_c<0~(n-1)>_wdrpro_strength" is 1
wdrc_mode <product dependent>	<boolean>	4/4	Enable WDR enhanced. * Only available when "capability_image_c<0~(n-1)>_wdrc_mode" is 1
wdrc_strength <product	1~100	4/4	The strength of WDR enhanced. The bigger value means the stronger

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
dependent>			strength of WDR enhanced. * Only available when "capability_image_c<0~(n-1)>_wdrc_mode" is 1
aespeed_mode <product dependent>	<boolean>	4/4	Turning AE converge speed on or off. 0: off 1: on * Only available when "capability_image_c<0~(n-1)>_aespeed" is 1
aespeed_speedlevel <product dependent>	1~100	4/4	The speed level of AE converge speed. 1~20: level 1 21~40: level 2 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)>_aespeed" is 1
aespeed_sensitivity <product dependent>	1~100	4/4	The sensitivity of AE converge speed. 1~20: level 1 21~40: level 2 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)>_aespeed" is 1 and

NAME	VALUE	SECURITY(get/set)	DESCRIPTION
			"capability_image_c<0~(n-1)>_aespeedsupportsensitivity" is 1.
flickerless <product dependent>	<boolean>	4/4	Turn on(1) or turn off(0) the flickerless mode * Only available when "capability_image_c<0~(n-1)>_flickerless" is 1.
mounttype	ceiling, wall, floor	1/6	Hardware installation. * Only available when "capability_videoin_c<0~(n-1)>_mounttype" != "-".
enablewatermark <product dependent>	0, 1	1/6	0: Not to add watermarks on images 1: Add watermarks on images * Only available when "capability_fisheye" > 0
s<0~(m-2)>_fisheyedewarpmode <product dependent>	'1O, 1P, 2P, 1R, 4R' for ceiling/floor mount '1O, 1P, 1R, 4R' for wall mount <product dependent>	1/4	Local dewarp mode. "1O" is original mode (disable). Supported dewarp mode is different by mount type. (videoin_c<0~(n-1)>_mounttype) Supported mode list could be extracted from (capability_videoin_c<0~(n-1)>_localdewarp_typeceilingmount) and (capability_videoin_c<0~(n-1)>_localdewarp_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"