FD360IR-E

High-Definition 6 MP

Fisheye Camera with D/N and IR

User Manual

Ver. 1.7

002B0XZXZ1A4

Note: To ensure proper operation, please read this manual thoroughly before using the product and retain the information for future reference.

Copyright © 2017 Siqura B.V.

FD360IR-E

User Manual v1.7 (151703-1.7)

MW10

Brand names

Any brand names mentioned in this manual are registered trademarks of their respective owners.

Liability

Siqura accepts no liability for claims from third parties arising from improper use other than that stated in this manual.

Although considerable care has been taken to ensure a correct and suitably comprehensive description of all relevant product components, this manual may nonetheless contain errors and inaccuracies. We invite you to offer your suggestions and comments by email via t.writing@tkhsecurity.com. Your feedback will help us to further improve our documentation.

How to contact us

If you have any comments or queries concerning any aspect related to the product, do not hesitate to contact:

Siqura B.V.

Zuidelijk Halfrond 4

2801 DD Gouda

The Netherlands

General : +31 182 592 333

Fax : +31 182 592 123

E-mail : sales.nl@tkhsecurity.com

WWW : www.siqura.com

Table of Contents

1. Overview

The FD360IR-E high-definition 6 MP fisheye camera is provided with a user-friendly browser-based configuration interface. This manual offers detailed information about the Home page, system settings, and camera settings.

For compliancy information, see the EU Declaration of Conformity, which is available for download at at www.tkhsecurity/support-files.

2. Menu Tree

There are five tabs on the Home Page: <Home>, <System>, <Streaming>, <Camera>, and <Logout>.

Home

Users can monitor live video of the targeted area on this page.

System

The administrator can set the host name, system time, root password, network related settings, etc. Further details are presented in the *System* chapter.

Streaming

The administrator can modify the video resolution and rotation type, and select an audio compression mode on this page.

Camera

The Camera tab is available to the administrator and user accounts that have been granted the privilege of camera control. On this tab, the administrator and users can adjust various camera parameters, including <Exposure>, <White Balance>, <Picture Adjustment>, <IR Function>, <Noise Reduction>, <Profile>, <Backlight>, <Digital Zoom>, <WDR Function>, , <Fisheye Setting>, and <TV System>.

Logout

Click the tab to log on to the camera with a different user name and password.

2.1 Home Page

Click the <**Home**> tab to access the home page. There are several function buttons on the home page. Detailed information of each item is given in the following section.

2.1.1 Function Items on the Home Page

Multiple Languages Support

Multiple languages are supported for the graphical user interface, including German, English, French, Italian, and Simplified Chinese.

Digital Zoom Control

In full screen mode, users can implement digital PTZ by rotating the mouse wheel (to zoom in/out) and dragging the mouse into any direction.

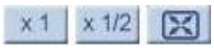
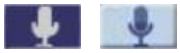
Screen Size Adjustment 

Image display size can be adjusted to x1/2 and full screen.

Talk button  (On/Off)

The Talk function allows the local site to talk to the remote site. Click the button to enable/disable the Talk function. See *Security> User> Add user> Talk / Listen* for further details.

NOTE: This function is available to users who have been granted this privilege by the administrator.

Speaker button  (On/Off)

Click the <Speaker> button to mute/activate the audio.

NOTE: This function is available to users who have been granted this privilege by the administrator.

Snapshot button 

Click the button and a JPEG snapshot is automatically saved to the designated location. The default storage location for snapshots is: C:\. To change the storage location, see section *File Location* for further details.

NOTE: Under the Windows 7 (or higher) operating system, to implement the Snapshot function, users must run IE as administrator.

To run IE as administrator, right-click the IE browser icon and then select “Run As Administrator” to launch IE.

Video Streaming Pause / Restart button  (Pause/Restart)

Click the <Stop> button to disable video streaming. The video preview goes blank. Click the <Restart> button to show live video again.

Web Recording button  (On/Off)

Click the <Recording> button and the Live View images from the web browser are directly recorded to the specified location on the local hard drive, which is configured on the <File Location> page. The default storage location for web recording is: C:\. See section *File Location* for further details.

NOTE: Under the Windows 7 (or higher) operating system, to implement the Web Recording function, users must run IE as administrator. To run IE as administrator, right-click the IE browser icon and then select “Run As Administrator” to launch IE.

Manual Trigger Button  (On/Off)

Click the <Manual Trigger > button to activate/deactivate the manual trigger. See section *Manual Trigger* of the next chapter for further details.

Fisheye Image Adjustment

- **Fisheye Source Image** 

  Click the <Fisheye Source Image> button to view live video as hemisphere fisheye source images.

- **Single view with ePTZ** 

  For a Ceiling Mount installed camera, click the <Single ePTZ> button to view the dewarped live images and virtually pan/tilt/zoom the camera according to your needs. Users can implement virtual PTZ by rotating the mouse wheel (to zoom in/out), and dragging the mouse into any direction.

- **360° Panoramic** 

  For a Ceiling Mount installed camera, click the <360° Panoramic> button to view the dewarped live images as two 180° views.

- **Quad View with ePTZ** 
  For a Ceiling Mount installed camera, click the <Quad View> button to view the dewarped live images as four ePTZ views.

- **180° Panoramic** 
  For a Wall Mount installed camera, click the <180° Panoramic> button to view the dewarped live video as a single 180° view.

- **Triple view with dual ePTZ** 
  For a Wall Mount installed camera, click the <Dual ePTZ> button to view the dewarped live video as a single 180° view with two ePTZ views. Users can implement virtual PTZ by rotating the mouse wheel (to zoom in/out), and drag the mouse into any direction in the ePTZ live video panes.

The available Fisheye Image Adjustment buttons are different according to the dewarping method and installation method selected on the <Fisheye Correction> setting page. The following table shows the available buttons in different dewarping methods and installation methods. The supported buttons are represented by "√".

Button \ Dewarping Method / Installation Method	Front End Correction*		Back End Correction	
	Ceiling Mount	Wall Mount	Ceiling Mount	Wall Mount
Fisheye Source Image	-	-	√	√
Single View with ePTZ	√**	-	√	-
360° Panoramic	√	-	√	-
Quad View with ePTZ	√	-	√	-
180° Panoramic	-	√	-	√
Triple view with dual ePTZ	-	√	-	√

*If users use the Front End Correction method for dewarping, the buttons are only shown when the video format is set to H.264-2 or MJPEG on the Home page.

**If users use the Front End Correction method, the Single ePTZ button supported in Ceiling Mount installation is only available when the resolution of the second stream is lower than "960 x 960".

2.2 System

On the <**System**> tab, there are submenus including: <System>, <Security>, <Network>, <DDNS>, <Mail>, <FTP>, <HTTP>, <Events>, <Storage Management>, <Recording>, <Schedule>, <File Location>, <View Information>, <Factory Default>, <Software Version>, <Software Upgrade>, and <Maintenance>.

NOTE: The <System> configuration page is accessible only to the administrator.

2.2.1 System

The System page can be found under the path: **System> System**.

Host Name

The host name is for camera identification. If the alarm function (see section *Application*) is enabled and set to send alarm message by Mail/FTP, the host name entered here is displayed in the alarm message. The maximum length of the Host Name is 63 characters.

Time Zone

Select the time zone in the drop-down list according to the location of the camera.

Enable Daylight Saving Time

To enable DST, select the item, and then specify the time offset and DST duration. The format for the time offset is [hh:mm:ss]. If, for example, the amount of time offset is one hour, enter “01:00:00” into the field.

Time format

Choose a time format (yyyy/mm/dd or dd/mm/yyyy) in the drop-down list. The format of the date and time displayed above the live video window is changed according to the selected format.

Sync with Computer Time

Select the item and the video date and time are synchronised with the PC date and time.

NOTE: Users *must* click the <Save> button to confirm the setting. Otherwise, the time is not synced.

Manual

Using this item, the administrator can set the video date and time manually. The entry format should be identical with the examples shown next to the text boxes.

Sync with NTP server

Using the Network Time Protocol (NTP) is an alternative method of synchronising the clock of the camera with an NTP server. In the text box, specify the server to be used for synchronising. Then select an update interval in the drop-down list. For further information about NTP, see www.ntp.org.

NOTE: The clock of the camera is synchronised every time the camera boots up.

Click <Save> to save the settings.

2.2.2 Security

The Security setting can be found under this path: **System> Security**.

Clicking <Security> opens a submenu with options including <User>, <HTTPS>, <IP Filter>, and <IEEE 802.1X>.

2.2.2.1 User

The User page can be found under this path: **System> Security> User**.

Admin Password

Use this section to change the administrator password. Enter the new password in <Admin password> and <Confirm password>. The maximum length is 14 characters. The input characters/numbers are displayed as dots for security purposes. Click <Save> to confirm the changes. After the changes are confirmed, the web browser prompts the administrator to log on to the camera with the new password.

 **NOTE:** The following characters are valid: A-Z, a-z, 0-9, !#$%&'-.@^_~.

Add User

Using this section, the administrator can add new users. Enter the new user name in <User name> and the password in <User password>. A user name can be up to 16 characters and the maximum length of the password is 14 characters. Select the boxes below to assign privileges for functions, including "**Camera control**", "**Talk**", and "**Listen**". Click <Add> to add the new user. The name of the newly added user is displayed in the <User name> list. There is a maximum of twenty user accounts.

- **I/O access**
  This item supports fundamental functions that enable users to view live video when they access the camera.

- **Camera control**
  This item allows the appointed user to change camera parameters on the camera setting page.

- **Talk/Listen**
  The Talk and Listen functions allow the appointed user in the local site (PC site) to communicate with, for example, the administrator in the remote site.

Manage User

- **Delete user**
  In the <User name> list, select the user name that is to be deleted. Click <Delete> to delete the selected user account.

- **Edit user**
  In the <User name> list, select the user that you wish to edit. Click <Edit> and a pop-up window appears. In this window, enter the new user password and change the privileges. Click <Save> to confirm the changes. Then click <Close> to complete the editing.

HTTP Authentication Setting

HTTP Authentication identifies whether a user is authorised to access the camera. Users are required to enter a valid user name and password before they can log on to the camera. Two types of authentication are available.

- **Basic**
  This type provides basic protection against unauthorised access. It is supported by most browsers. Note that passwords are sent over the network in clear text. If intercepted they can be reused by unauthorised users. Select this type only if you are using an SSL connection or a dedicated line.
- **Digest**
  This type is a more secure option. It encrypts the password before sending it over the network.

Streaming Authentication Setting

This setting provides security against unauthorised users attempting to open a stream via the Real Time Streaming Protocol (RTSP). If the setting is enabled, users are required to enter their user name and password before viewing the live streams. There are three security modes available: Disable, Basic and Digest.

- **Disable**
  If the disable mode is selected, no security is provided to prevent unauthorised access. Users are not asked to provide their user name and password for authentication.

- **Basic**
  This mode provides basic protection for the live streams. There is still the risk of the password being intercepted.

- **Digest**
  Digest mode is a safer option for protection. The password is sent in an encrypted format to prevent it from being stolen.

NOTE: Users *must* click the <Save> button to apply the setting.

2.2.2.2 HTTPS

The HTTPS setting can be found under this path: **System> Security> HTTPS**.

HTTPS allows secure connections between the IP camera and web browser using <Secure Socket Layer (SSL)> or <Transport Layer Security (TLS)>, which protect camera settings or user name / password info against snooping. To implement HTTPS, a self-signed certificate or a CA-signed certificate must be installed.

To use HTTPS on the IP camera, an HTTPS certificate must be installed. The HTTPS certificate can be obtained by either creating and sending a certificate request to a Certificate Authority (CA) or creating a self-signed HTTPS certificate, as described below.

Create Self-signed Certificate

Before a CA-issued certificate is obtained, users can create and install a self-signed certificate.

Click <Create> and provide the information required to install a self-signed certificate for the camera. See the last part of the *Provide the Certificate Information* section for more details.

NOTE: The self-signed certificate does not provide the same high level of security as the CA-issued certificate.

Install Signed Certificate

Click the <Create Certificate Request> button to create and submit a certificate request in order to obtain a signed certificate from a CA.

Provide the request information in the create dialogue. See the following section *Provide the Certificate Information* for more details.

When the request is complete, the subject of the Created Request is shown in the text box. Click <Properties> below the Subject box, copy the PEM-formatted request, and then send it to the selected CA.

When the signed certificate is returned, install it by uploading the signed certificate.

Provide the Certificate Information

To create a Self-signed HTTPS Certificate or a Certificate Request to CA, enter the information as requested.

	Create Self Signed Certificate	Create Certificate Request
Country	√	√
State or Province	√	√
Locality	√	√
Organisation	√	√
Organisational Unit	√	√
Common Name	√	√
Valid Day	√	-

- **Country**
  Enter a two-letter code to indicate the country that the certificate will be used in. For example, type “US” to indicate the United States.

- **State or province**
  Enter the local administrative region.

- **Locality**
  Enter other geographical information.

- **Organisation**
  Enter the name of the organisation to which the entity identified in “Common Name” belongs.

- **Organisation Unit**
  Enter the name of the organisational unit to which the entity identified in “Common Name” belongs.

- **Common Name**
  Indicate the name of the person or other entity that the certificate identifies (often used to identify the website).

- **Valid days**
  Enter the period in days (1 to 9999) to indicate the valid period of the certificate.

Click <OK> to save the Certificate Information after completion.

2.2.2.3 IP Filter

The IP Filter setting can be found under this path: **System> Security> IP Filter**.

With the IP Filter function, users can allow or deny access to the camera from specific IP addresses.

- **Enable IP Filter**
  Select the box to enable the IP Filter function. Once enabled, the listed IP addresses (IPv4) in the <Filtered IP Addresses> list box are allowed/denied access to the camera.

  Click <Allow> or <Deny> in the drop-down list and click on the <Apply> button to determine the IP filter behaviour.

- **Add IP Address**
  Type the IP address in the text box under the <Filtered IP Address> list and click <Add>. The newly added address is shown in the list. Up to 256 IP addresses can be specified.

  To filter a group of IP addresses, type an address in the text box, followed by a slash and a number ranging from 1 to 31, such as 192.168.2.81/30, for example. The number after the slash defines how many IP addresses will be filtered. For details, see the following example.

- **Example:** Filtering a group of consecutive IP addresses
  The steps below show what is filtered when 192.168.2.81/30 is entered.

  Step 1: Convert 192.168.2.81 to binary format. The binary digits are 11000000.10101000.00000010.01010001. See *Appendix B: IP Addresses from Decimal to Binary* for conversion of IP addresses to binary format. The number "30" after the slash refers to the first 30 digits of the binary number.

  Step 2: Convert a few IP addresses before and after 192.168.2.81 to binary format. Then compare their first 30 digits to the binary format of 192.168.2.81.

  a. Convert 192.168.2.80 to binary. The binary representation is 11000000.10101000.00000010.01010000. The first 30 digits are the same as the binary digits of 192.168.2.81. Therefore 192.168.2.80 is filtered.

  b. Convert 192.168.2.79 to binary. The binary representation is 11000000.10101000.00000010.01001111. The first 30 digits are different from the binary digits of 192.168.2.81. Therefore, 192.168.2.79 is not filtered. This also means that the IP addresses preceding 192.168.2.79 are not filtered.

  c. Repeat the procedure given in a" with the IP addresses following 192.168.2.81. Stop when the situation described in "b" occurs – that is, the 30th digit of the binary format of IP address 192.168.2.84 is different, and is not filtered.

  As a result, the IP addresses 192.168.2.80 to 192.168.2.83 are filtered when entering 192.168.2.81/30. The following table clearly shows that the 30th digit of the binary format of IP addresses 192.168.79 and 192.168.84 differ from the others. Therefore, these two IP addresses are not filtered.

IP Addresses	Binary Numbers
192.168.2.79	**11000000.10101000.00000010.01001111**
192.168.2.80	**11000000.10101000.00000010.01010000**
192.168.2.81	**11000000.10101000.00000010.01010001**
192.168.2.82	**11000000.10101000.00000010.01010010**
192.168.2.83	**11000000.10101000.00000010.01010011**
192.168.2.84	**11000000.10101000.00000010.01010100**

- **Delete IP Address**
  To remove an IP address from the list, select the IP, and then click <Delete>.

2.2.2.4 IEEE 802.1X

The IEEE 802.1X setting can be found under this path: **System> Security> IEEE 802.1X**.

The camera is allowed to access a network protected by 802.1X/EAPOL (Extensible Authentication Protocol over LAN).

Users need to contact the network administrator to obtain certificates, user IDs, and passwords.

CA Certificate

A CA certificate is created by a Certification Authority for validation purposes. Upload the certificate to check the server's identity.

Client Certificate / Private Key

Upload the Client Certificate and Private Key to authenticate the camera itself.

Settings

- **Identity**
  Enter the user identity associated with the certificate. Up to 16 characters can be used.

- **Private Key Password**
  Enter the password (maximum 16 characters) associated with the user identity.

Enable IEEE 802.1X

Select the box to enable IEEE 802.1X.

Click <Save> to save the IEEE 802.1X/ EAP- TLS setting.

2.2.3 Network

The Network settings can be found under this path: **System> Network**.

Clicking <Network> opens a submenu with options including <Basic>, <QoS>, <SNMP>, and <UPnP>.

2.2.3.1 Basic

Basic settings can be found under this path: **System> Network> Basic**.

Use this page to set a new IP address for the camera, configure other network-related parameters, and activate the IPv6 address (if the network supports this).

General

This section is for configuring a new IP address for the camera. To assign an IP address, contact the network provider to find out the network type first. Then refer to the network type and follow the instructions to set up the IP address.

NOTE: If the network type is Point-to-Point Protocol over Ethernet (PPPoE), obtain the PPPoE username and password from the network provider.

- **Get IP address automatically (DHCP)**
  Click the item and then click <Save> to confirm the new setting. A notice about a camera system restart appears. Click <OK> and the camera system is restarted. A new IP address is assigned to the camera. Close the web browser and search the camera through Device Manager. With Device Manager - a tool that you can download at www.tkhsecurity/support-files - you can locate, manage, and configure TKH Security IP cameras and video encoders.

  NOTE: Before searching the camera through Device Manager, record the MAC address of the camera for later use and identification. It can be found on the label or on the package container of the camera.

Step 1: Download Device Manager, double-click the setup file, and follow the installation steps to install the software.

Step 2: Start Device Manager, wait while the network is scanned. Detected devices appear in the List View pane. If multiple network adapters exist, select the appropriate adapter to scan the network you wish to connect to. To perform a manual search, click the *Rescan* button. Use the tabs in the *Tree View* pane to define the scope of your search. Click the column headings in the *List View* pane to sort devices by type, IP address, or name.

Step 3: To connect to the webpages of the camera, double-click its entry in the device list, or right-click the entry, and then click *Open Web Page*.

Step 4: To directly change the network settings of the camera with Device Manager, go to the list of detected devices, and then right-click the entry for the camera. Click *Change Network Settings*, click *Enable DHCP*, and then click *OK.* Wait one minute, and then rescan the network. You can identify the camera by its MAC address.

Step 5: To access the webpages of the camera, double-click its entry in the list of found devices.

NOTE: A DHCP server must be installed on the network in order to provide DHCP network support.

- **Use fixed IP address**

  Click the item and enter the new IP address. Note that the specified IP address and the IP address of the PC should be in the same subnet. Enter the IP address of the Default gateway (explained later) as required. Click <Save> to confirm the new setting. A notice about a camera system restart appears. Click <OK> and the system restarts. Wait for 15 seconds. The camera's IP address in the URL bar is changed and the user has to log on again.

  When using a fixed IP address to connect the camera, users can access the camera by typing the IP address in the URL bar and pressing <Enter> on the keyboard. Alternatively, users can access the camera with Device Manager, as described in the previous section.

To assign a fixed IP address through Device Manager, right-click the camera entry in the list of detected devices, click *Change Network Settings*, and then click *Static IP*. You can then provide the camera with an appropriate IP address, netmask, and gateway address for the desired network configuration.

- IP address
  This is necessary for network identification.

- Subnet mask
  This is used to determine if the destination is in the same subnet. The default value is “255.255.255.0”.

- Default gateway
  This is the gateway used to forward frames to destinations in different subnets. An invalid gateway setting prevents transmissions to destinations in different subnets.

- Primary DNS
  Primary DNS is the primary domain name server that translates host names into IP addresses.

- Secondary DNS
  Secondary DNS is a secondary domain name server that backs up the primary DNS.

- **Use PPPoE**
  For PPPoE users, enter the PPPoE user name and password into the text boxes, and click <Save> to complete configuring the setting.

Advanced

This section describes the Web Server port, RTSP port, MJPEG over HTTP port, and HTTPS port settings.

- **Web Server port**
  The default web server port is 80. With the default web server port set to '80', users can simply enter the IP address of the camera in the URL bar of a web browser to connect to the camera. If the web server port is changed to any number other than 80, users have to enter the camera's IP address followed by a colon and the port number. For example, a camera with IP address 192.168.0.100 and web server port 8080 can be accessed by entering "http://192.168.0.100:8080" in the URL bar.

- **RTSP port**
  The default setting of RTSP Port is 554; the setting range is from 1024 to 65535.

- **MJPEG over HTTP port**
  The default setting of MJPEG over HTTP Port is 8008; the setting range is from 1024 to 65535.

- **HTTPS port**
  The default setting of HTTPS Port is 443; the setting range is from 1024 to 65535.

NOTE: Make sure that the port numbers set above are unique, otherwise a network conflict may occur.

IPv6 Address Configuration

If the network supports IPv6, users can select the <Enable IPv6> check box and click <Save>. An IPv6 address is displayed next to <Address> and users can use it to connect to the camera.

2.2.3.2 QoS

The QoS (Quality of Service) setting can be found under this path: **System> Network> QoS**.

QoS allows providing differentiated service levels for different types of traffic packets, which guarantees delivery of priority services especially when network congestion occurs. Adapting the Differentiated Services (DiffServ) model, traffic flows are classified and marked with DSCP (DiffServ Codepoint) values, and thus receive the corresponding forwarding treatment from DiffServ capable routers.

DSCP Settings

The DSCP value range is from 0 to 63. The default DSCP value is 0, which means DSCP is disabled. The camera uses the following QoS Classes: Video, Audio, and Management.

- **Video DSCP**
  This class applies to applications such as MJPEG over HTTP, RTP/RTSP, and RTSP/HTTP.

- **Audio DSCP**
  This setting is available for IP cameras which support audio.

- **Management DSCP**
  This class applies to HTTP traffic: Web browsing.

NOTE: To enable this function, make sure the switches/routers in the network support QoS.

2.2.3.3 SNMP

The SNMP (Simple Network Management Protocol) setting can be found under this path: **System> Network> SNMP**.

With Simple Network Management Protocol (SNMP) support, the IP camera can be monitored and managed remotely by the network management system.

SNMP v1/v2

- **Enable SNMP v1/v2**
  Select the version of SNMP to use by selecting the box.

- **Read Community**
  Specify the community name that has read-only access to all supported SNMP objects. The default value is “public”.

- **Write Community**
  Specify the community name that has read/write access to all supported SNMP objects (except read-only objects). The default value is “private”.

SNMP v3

SNMP v3 supports an enhanced security system that provides protection against unauthorised users and ensures the privacy of the messages. Users are requested to enter a security name, authentication password, and encryption password when setting the camera connections in the network management system. With SNMP v3, the messages sent between the cameras and the network management system are encrypted to ensure privacy.

- **Enable SNMP v3**
  Enable SNMP v3 by selecting the box.

- **Security Name**
  The maximum length of the security name is 32 characters.

  NOTE: Valid characters are A-Z, a-z, 0-9, !#$%&’-.@^_~.

- **Authentication Type**
  Two authentication types are available: MD5 and SHA. Select SHA for a higher security level.

- **Authentication Password**
  The authentication password must be eight characters or more. The input characters/numbers are displayed as dots for security purposes.

  NOTE: Valid characters are A-Z, a-z, 0-9, !#$%&'-.@^_~.

- **Encryption Type**
  Two encryption types are available: DES and AES. Select AES for a higher security level.

- **Encryption Password**
  The minimum length of the encryption password is eight characters and the maximum length is 512 characters. The input characters/numbers are displayed as dots for security purposes. The encryption password can also be left blank. In that case, the messages are not encrypted to protect privacy.

  NOTE: Valid characters are A-Z, a-z, 0-9, !#$%&'-.@^_~.

Traps for SNMP v1 / v2 / v3

Traps are used by the camera to send messages to a management system on important events or status changes.

- **Enable Traps**
  Select the box to activate trap reporting.

- **Trap address**
  Enter the IP address of the management server.

- **Trap community**
  Enter the community to use when sending a trap message to the management system.

Trap Option

- **Warm Start**
  A Warm Start SNMP trap signifies that the SNMP device, such as the IP camera, reinitialises itself by performing a software reload.

Click <Save> when finished.

2.2.3.4 UPnP

The UPnP setting can be found under this path: **System> Network> UPnP**.

UPnP Setting

- **Enable UPnP**
  If enabled, UPnP allows the camera to advertise its presence and services to control points (for example, a VMS) on the network. The icon of the connected camera appears in My Network Places to allow direct access.

  NOTE: To enable this function, make sure that UPnP is installed on the computer. See *Appendix A: Install UPnP components* for the UPnP installation procedure.

- **Enable UPnP port forwarding**
  When UPnP port forwarding is enabled, the IP camera is allowed to open the web server port on the router automatically.

  NOTE: To enable this function, make sure that the router supports UPnP and that it is activated.

- **Friendly name**
  Set the name that the IP camera will use to identify itself on the network

Click <Save> when finished.

2.2.4 DDNS

The DDNS setting can be found under this path: **System> DDNS**.

The Dynamic Domain Name System (DDNS) allows a host name to be constantly synchronised with a dynamic IP address. In other words, it allows those using a dynamic IP address to be associated with a static domain name, so that others can connect to it by name.

Enable DDNS
Select the item to enable DDNS.

Provider
Select one DDNS host from the provider list.

Host name
Enter the registered domain name in the field.

Username/E-mail
Enter the user name or email required by the DDNS provider for authentication.

Password/Key
Enter the password or key required by the DDNS provider for authentication.

Click <Save> when finished.

2.2.5 Mail

The Mail setting can be found under this path: **System> Mail**.

The administrator can send an email via Simple Mail Transfer Protocol (SMTP) when event is triggered. SMTP is a protocol for sending email messages between servers. SMTP is a relatively simple, text-based protocol, where one or more recipients of a message are specified and the message text is transferred.

Two sets of SMTP can be configured. Each set includes SMTP Server, Server Port, Account Name, Password and Email Address settings. Select the box “SMTP SSL” to send emails via encrypted transmission. For SMTP server details, contact the network service provider for more specific information.

Click <Save> when finished.

2.2.6 FTP

The FTP setting can be found under this path: **System> FTP**.

The administrator can configure the camera to send an alarm message to up to two FTP sites. Enter the FTP details, which include a server, server port, user name, password and remote folder. Select the box “passive mode” to be connected with the FTP server by passively receiving the FTP server’s IP address through a dynamic port. Alternatively, clear the box to directly connect to the FTP server via active mode.

Click <Save> when finished.

2.2.7 HTTP

The HTTP setting can be found under this path: **System> HTTP**.

An HTTP Notification server can listen for notification messages from IP cameras triggered by events. Enter the HTTP details, which include a server name (for example, http://192.168.0.1/admin.php), user name, and password. <Alarm> triggered and <Motion Detection> notifications can be sent to the specified HTTP server.

Click <Save> when finished.

See *Events> Application> Send HTTP notification / Motion Detection* for HTTP Notification settings.

2.2.8 Events

The Events setting can be found under this path: **System> Events**.

Clicking the Events menu opens a submenu with options including <Application>, <Motion Detection>, <Network Failure Detection>, <Tampering>, <Periodical Event>, <Manual Trigger>, and <Audio Detection>.

2.2.8.1 Application

The Application setting can be found under this path: **System> Events> Application**.

The camera supports one alarm input and one relay output to be used with an alarm system to catch event images. See the alarm pin definition below to connect alarm devices to the camera if needed.

Alarm Pin Definition

Refer to the Installation Manual available at www.tkhsecurity/support-files for the Alarm Pin Definition when connecting alarm devices to the camera.

Alarm Switch

The default setting for the Alarm Switch function is <Off>. Enable the function by selecting <On>. Users can also activate the function according to the schedule previously set on the <Schedule> setting page. Select <By schedule> and click <Please select…> to choose the desired schedule from the drop-down menu.

Alarm Type

Select an alarm type, <Normal close> or <Normal open>, that corresponds with the alarm application.

Alarm Output

Select alarm output signal <high> or <low> as the normal alarm output status according to the current alarm application.

Triggered Action (Multi-option)

The administrator can specify alarm actions to be performed when the alarm is triggered.

- **Enable Alarm Output**
  Select the item to enable alarm relay output.

- **IR Cut Filter**
  Select the item to have the IR cut filter (ICR) of the camera removed (on) or blocked (off) when the alarm input is triggered.

  Note: The IR Function (See section *IR Function*) cannot be set to <Auto> if this triggered action is enabled.

- **Send Message by FTP/E-Mail**
  The administrator can select whether to send an alarm message by FTP and/or email when an alarm is triggered.

- **Upload Image by FTP**
  Select this item and the administrator can assign an FTP site and configure various parameters. When the alarm is triggered, event images are uploaded to the appointed FTP site.

  The <Pre-trigger buffer> function allows users to check what caused the trigger. The number of <Pre-trigger buffer> frames can be predetermined. The <Post-trigger buffer> can be used to upload a certain amount of images after the alarm input is triggered.

  NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

Select the box <Continue image upload> to upload the triggered images for the specified time or to keep uploading until the trigger is off. Select <Upload for __ sec> and enter the duration in the blank. The images are uploaded to FTP for the set duration when the alarm input is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue image upload to FTP during the trigger active until the alarm is released. Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

NOTE: Make sure that the FTP settings have been correctly configured. See section *FTP* for further details.

- **Upload Image by E-Mail**

  Select this item and the administrator can assign an email address and configure various parameters. When the alarm input is triggered, event images are sent to the appointed email address.

  The <Pre-trigger buffer> function allows users to check what caused the trigger. The number of <Pre-trigger buffer> frames can be predetermined. The <Post-trigger buffer> can be used to upload a certain amount of images after the alarm input is triggered.

  NOTE: Normally the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

  Select the box <Continue image upload> to upload the triggered images for the specified time or to keep uploading until the trigger is off. Select <Upload for __ sec> and enter the duration in the blank. The images are uploaded to FTP for the set duration when the alarm input is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue image upload to FTP during the trigger active until the alarm is released. Set the Image frequency as the upload frame rate. The setting range is from 1 frame to 15 frames.

  NOTE: Make sure that the SMTP settings have been correctly configured. See section *Mail* for further details.

- **Send HTTP notification**
  Select this item and select the destination HTTP address. Then specify the parameters for event notifications in the Custom parameters box. When an alarm is triggered, the HTTP notification is sent to the specified HTTP server.

  For example, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.1/admin.php”, the notification is sent to the HTTP server as “http://192.168.0.1/admin.php?action=1&group=2” when an alarm is triggered.

- **Record Video Clip**
  Select this item and then select a video recording storage type, <SD Card> or <NAS> (Network-Attached Storage). The alarm-triggered recording will be saved to the microSD card or the NAS.

  The <Pre-trigger buffer> recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 seconds.

  Select <Upload for __ sec> to set the recording duration after the alarm is triggered. The setting range is from 1 to 99999 seconds. Select <Upload during the trigger active> to continue recording the triggered video until the trigger is off.

  NOTE: Make sure that local recording (with microSD/SDHC card) or remote recording (with NAS) is activated so that this function can be implemented. See section *Recording* for further details.

File Name

Enter a file name in the box. The file name format of the uploaded image can be set in this section. Select the one that meets the requirements.

- **Add date/time suffix**
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number

- **Add sequence number suffix (no maximum value)**
  File name: imageXXXXXXX.jpg
  X: Sequence Number

- **Add sequence number suffix up to # and then start over**
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ranges up to the set number. For example, if the setting is up to “10”, the file name starts at 00, ranges to 10, and then starts all over.

- **Overwrite**
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Save

After completing the settings above, click <Save> to save the settings on this page.

2.2.8.2 Motion Detection

The Motion Detection settings can be found under this path: **System> Events> Motion Detection**.

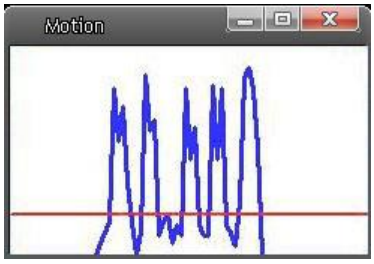
The Motion Detection function allows detecting suspicious motion and triggering alarms when the motion volume in the detected area reaches/exceeds the determined sensitivity threshold value.

The function supports up to four sets of Motion Detection settings. Settings can be chosen from the <Motion Detection> list. In each set of settings, there is a **Motion Detection Window** (the red frame shown in the figure below) displayed on the Live Video pane. The Motion Detection Window is for defining the motion detection area. To change the size of the Motion Detection Window, move the mouse cursor to the edge of the window and drag it outward/inward. To shift the window to the intended location, move the mouse cursor to the centre of the window and then click and drag.

Users can configure up to 10 sets of Motion Detection Windows in each set of Motion Detection settings. Click on the <add> button under the Live Video pane to add a Motion Detection Window. To delete a Motion Detection Window, move the mouse cursor to the selected window, and click the <delete> button.

When Motion Detection function is activated, the pop-up window (Motion) with indication of motion is shown.

When motion is detected, the signals are displayed on the Motion window as shown below. Motion is detected by comparing sampling pixels in the detection area of two consecutive live images.



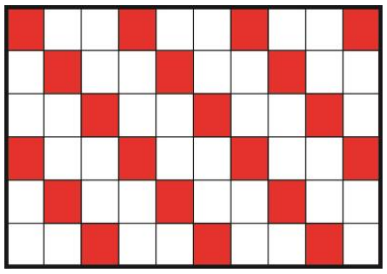
Motion Detection

In each set of Motion Detection settings, the default setting for the Motion Detection function is <Off>. Enable the function by selecting <On>. Users can also activate the function according to a schedule previously set on the <Schedule> setting page. Select <By schedule> and click <Please select…> to choose the desired schedule from the drop-down menu.

Motion Detection Setting

Users can adjust various Motion Detection parameters in this section.

- **Sampling pixel interval [1-10]:**
  Users can define the intervals between the sampling pixels here. The default value is 1. If the value is set to 3, the system takes the first pixel out of every 3 pixels per row and per column in the detection region, as a sample.



- **Detection level [1-100]:**
  Use this item to set the detection level for each sampling pixel. The smaller the value, the more sensitive it is. The default level is 10.

- **Sensitivity level [1-100]:**
  The default level is 80, which means that if 20% or more sampling pixels in the detection window change, the system will detect motion. The higher the value, the more sensitive it is. As the value increases, the red horizontal line in the motion indication is lowered accordingly.

- **Time interval (sec) [0-7200]:**
  The value is the interval between each detected motion. The default interval is 10.

<u>Triggered Action</u> (Multi-option)
The administrator can specify alarm actions to be performed when motion is detected.

- **Enable Alarm Output**
  Select the item and then select the predefined type of alarm output to enable alarm relay output when motion is detected.

- **Record Video Clip**
  Select this item and then select a video recording storage type, <SD Card> or <NAS> (Network-Attached Storage>. The Motion Detection recording is stored on the microSD/SDHC card or the NAS when motion is detected.

  The <Pre-trigger buffer> recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 seconds. Select <Upload for __ sec> to set the recording duration after the motion event occurs. The setting range is from 1 to 99999 seconds.

  Select <Upload during the trigger active> to record the triggered video until the trigger is off.

  NOTE: Make sure that the local recording (with microSD/SDHC card) or the remote recording (with NAS) is activated so that this function can be implemented. See section *Recording* for further details.

- **Send Alarm Message by FTP/E-Mail**
  The administrator can select whether to send warning messages by FTP and/or email when motion is detected.

- **Upload Image by FTP**
  Select this item and the administrator can assign an FTP site and configure various parameters. When motion is detected, event images are uploaded to the appointed FTP site.

  The <Pre-trigger buffer> function allows users to check what caused the trigger. The number of <Pre-trigger buffer> frames can be predetermined. The <Post-trigger buffer> can be used to upload a certain amount of images after the alarm input is triggered.

  NOTE: Normally the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

  Check the box <Continue image upload> to upload the triggered images for a certain time or to continue uploading until the trigger is off. Select <Upload for __ sec> and enter the duration in the blank. The images are uploaded to FTP for the duration when the motion event occurs. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue the image upload to FTP during the trigger active until the event stops. Set the Image frequency by selecting an upload frame rate. The setting range is from 1 frame to 15 frames.

  NOTE: Make sure that the FTP settings have been correctly configured. See section *FTP* for further details.

- **Upload Image by E-Mail**
  Select this item and the administrator can assign an email address and configure various parameters. When motion is detected, event images are sent to the appointed email address.

  The <Pre-trigger buffer> function allows users to check what caused the trigger. The number of <Pre-trigger buffer> frames can be pre-determined. The <Post-trigger buffer> can be used to upload a certain amount of images after the motion event occurs.

  NOTE: Normally the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

  Check the box <Continue image upload> to upload the triggered images for a certain time or to continue uploading until the trigger is off. Select <Upload for __ sec> and enter the duration in the box. Images are uploaded by email for the specified duration when the motion event occurs. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue the image upload by email during the trigger active until the event stops. Set the number of frames for the Image frequency. The setting range is from 1 frame to 15 frames.

  NOTE: Make sure that the SMTP settings have been correctly configured. See section *Mail* for further details.

- **Send HTTP notification**
  Select this item and then select the destination HTTP address. Use the Custom parameters box to specify the parameters for event notifications. When motion is detected, the HTTP notification is sent to the specified HTTP server.

  For example, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.1/admin.php”, the notification is sent to HTTP server as “http://192.168.0.1/admin.php?action=1&group=2” when an alarm is triggered.

File Name

Enter a file name in the box. The file name format of the uploaded image can be set in this section. Select the one that meets the requirements.

- **Add date/time suffix**
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number

- **Add sequence number suffix (no maximum value)**
  File name: imageXXXXXXX.jpg
  X: Sequence Number

- **Add sequence number suffix up to # and then start over**
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ranges up to the set number. For example, if the setting is up to “10”, the file name starts at 00, ranges up to 10, and then starts all over.

- **Overwrite**
  The original image in the FTP site will be overwritten by the new uploaded file with a static filename.

Save

Click the <Save> button to save the Motion Detection settings mentioned above.

2.2.8.3 Network Failure Detection

The Network Failure Detection setting can be found under this path: **System> Events> Network Failure Detection**.

Network Failure Detection allows the IP camera to periodically ping another IP device (e.g. an NVR, VSS, Video Server, etc.) within the network and generate some actions in case a network failure occurs; for example, when a Video Server is disconnected somehow.

Being capable of implementing local recording (through the microSD card) or remote recording (via NAS) when network failure happens, the camera can be a backup recording device for the surveillance system.

Detection Switch

The default setting for the Detection Switch function is <Off>. Enable the function by selecting <On>. Users can also activate the function according to a time schedule that was previously set on the <Schedule> setting page. Select <By schedule> and then click <Please select…> to choose the desired schedule from the drop-down list.

Detection Type

Enter the device IP address and the ping time interval. Ping time setting ranges from 1 to 99 minutes.

Triggered Action (Multi-option)

The administrator can specify alarm actions to be performed when network failure is detected.

- **Enable Alarm Output**
  Select the item to enable alarm relay output.

- **Record Video Clip**
  Select the item and then select a video recording storage type, <SD Card> or <NAS> (Network-Attached Storage). The alarm-triggered recording is saved to the microSD card or the NAS.

  The <Pre-trigger buffer> recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 seconds. Select <Upload for __ sec> to set the recording duration after the alarm is triggered. The setting range is from 1 to 99999 seconds.

Select <Upload during the trigger active> to record the triggered video until the trigger is off.

NOTE: Make sure that local recording (with microSD/SDHC card) or remote recording (with NAS) is activated so that this function can be implemented. See section *Recording* for further details.

- **Send Alarm Message by FTP/E-Mail**
  The administrator can select whether to send an alarm message by FTP and/or email when an alarm is triggered.

Save

Click <Save> to save all the settings mentioned above.

2.2.8.4 Tampering

The Tampering setting can be found under this path: **System> Events> Tampering**.

The Tampering Alarm function enables the IP camera to detect tampering, such as deliberate redirection, blocking, paint spraying, and lens covering, etc, through video analysis and to react to such events by sending out notifications or uploading snapshots to the specified destination(s).

Detection of camera tampering is achieved by measuring the differences between previous frames of video (stored in buffers) and more recent frames.

Tampering Alarm

The default setting for the Tampering Alarm function is <Off>. Enable the function by selecting <On>. Users can also activate the function according to a schedule previously set on the <Schedule> setting page. Select <By schedule> and then click <Please select…> to choose the desired schedule from the drop-down list.

Tampering Duration

The Minimum tampering duration is the time for video analysis to determine whether camera tampering has occurred. The Minimum duration can also be interpreted as the Tampering threshold; a longer duration represents a higher threshold. The configurable Tampering Duration ranges from 10 to 3600 seconds. The Default value is 20 seconds.

Triggered Action (Multi-option)

The administrator can specify alarm actions to be performed when tampering is detected.

- **Enable Alarm Output**
  Select the item and then select the predefined type of alarm output to enable alarm output when tampering is detected.

- **Record Video Clip**
  Select this item and then select a video recording storage type, <SD Card> or <NAS> (Network-Attached Storage). The alarm-triggered recording is stored on the microSD/SDHC card or the NAS.

The <Pre-trigger buffer> recording function allows users to check what caused the trigger. The pre-trigger buffer time ranges from 1 to 3 seconds. Select <Upload for __ sec> to set the recording duration after tampering occurs. The setting range is from 1 to 99999 seconds. Select <Upload during the trigger active> to record the triggered video until the trigger is off.

NOTE: Make sure that local recording (with microSD/SDHC card) or remote recording (with NAS) is activated so that this function can be implemented. See section *Recording* for further details.

- **Send Message by FTP/E-Mail**
  The administrator can select whether to send an alarm message by FTP and/or email when tampering is detected.

- **Upload Image by FTP**
  Select this item and the administrator can assign an FTP site and configure various parameters. When tampering is detected, event images are uploaded to the appointed FTP site.

  The <Pre-trigger buffer> function allows users to check what caused the trigger. The number of <Pre-trigger buffer> frames can be predetermined. The Post-trigger buffer> can be used to upload a certain amount of images after tampering has been detected.

  NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

  Select the box <Continue image upload> to upload the triggered images for a certain time or to continue uploading until the trigger is off. Select <Upload for __ sec> and enter the duration in the box. The images are uploaded to FTP for the set duration when tampering is detected. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue the image upload to FTP during the trigger active – that is, until the tampering stops. Set the Image frequency by selecting an upload frame rate. The setting range is from 1 to 15 frames.

NOTE: Make sure that the FTP configuration has been completed. See section *FTP* for further details.

- **Upload Image by E-Mail**
  Select this item and the administrator can assign an email address and configure various parameters. When tampering is detected, event images are sent to the appointed email address.

  The <Pre-trigger buffer> function allows users to check what caused the trigger. The <Pre-trigger buffer> frame rate can be predetermined. The, <Post-trigger buffer> can be used to upload a certain amount of images after tampering occurs.

  NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

  Check the box <Continue image upload> to upload the triggered images for a certain time or to continue uploading until the trigger is off. Select <Upload for __ sec> and enter the duration in the box. The images are uploaded by email for the set duration when tampering is detected. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue the image upload to email during the trigger active – that is, until tampering stops. Set the Image frequency by selecting an upload frame rate. The setting range is from 1 to 15 frames.

  NOTE: Make sure that the SMTP configuration has been completed. See section *Mail* for further details.

- **Send HTTP notification**
  Select this item and then select the destination HTTP address. Specify the parameters for HTTP notifications. When the Tampering Alarm is triggered, the HTTP notifications can be sent to the specified HTTP server.

  For example, if the custom parameter is set as “action=1&group=2”, and the HTTP server name is “http://192.168.0.1/admin.php”, the notification is sent to the HTTP server as “http://192.168.0.1/admin.php?action=1&group=2” when an alarm is triggered.

File Name

Enter a file name in the box. The file name format of uploaded images can be set in this section. Select the one that meets the requirements.

- **Add date/time suffix**
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number

- **Add sequence number suffix (no maximum value)**
  File name: imageXXXXXXX.jpg
  X: Sequence Number

- **Add sequence number suffix up to # and then start over**
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ranges up to the set number. For example, if the setting is up to “10”, the file name starts at 00, ranges up to 10, and then starts all over.

- **Overwrite**
  The original image in the FTP site will be overwritten by the newly uploaded file with a static filename.

Save

Click <Save> to save all the settings mentioned above.

2.2.8.5 Periodical Event

The Periodical Event setting can be found under this path: **System> Events> Periodical Event**.

Using the Periodical Event setting, users can set the camera to upload images periodically to an FTP site or an email address. For example, if the time interval is set to 60 seconds, the camera uploads images to the assigned FTP site or email address every 60 seconds. The images to be uploaded are the images before and after the triggered moment. Users can define the number of images to be uploaded in the <Triggered Action> section of this setting page.

Periodical Event

The default setting for the Periodical Event function is <Off>. Enable the function by selecting <On>.

Time Interval

The default value of the time interval is 60 seconds. The setting range of the time interval is from 60 to 3600 seconds.

Triggered Action

- **Upload Image by FTP**
  Select this item and the administrator can assign an FTP site and configure various parameters. Images will be periodically uploaded to the appointed FTP site.

  The <Pre-trigger buffer> function defines the number of images to be uploaded before the triggered moment. The <Post-trigger buffer> function defines the number of images to be uploaded after the triggered moment.

  NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

  NOTE: Make sure that the FTP configuration has been completed. See the *FTP* section of this chapter for further details.

- **Upload Image by E-Mail**
  Select this item and the administrator can assign an email address and configure various parameters. Images are uploaded to the appointed email address periodically.

  The <Pre-trigger buffer> function defines the number of images to be uploaded before the triggered moment. The <Post-trigger buffer> function defines the number of images to be uploaded after the triggered moment.

  NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

  NOTE: Make sure that the SMTP configuration has been completed. See the *Mail* section of this chapter for further details.

File Name

Enter a file name in the box. The file name format of uploaded images can be set in this section. Select the one that meets the requirements.

- **Add date/time suffix**
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number

- **Add sequence number suffix (no maximum value)**
  File name: imageXXXXXXX.jpg
  X: Sequence Number

- **Add sequence number suffix up to # and then start over**
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix ranges up to the set number. For example, if the setting is up to “10”, the file name starts at 00, ranges up to 10, and then starts all over.

- **Overwrite**
  The original image in the FTP site will be overwritten by the newly uploaded file with a static filename.

Save

Click <Save> to save all the settings mentioned above.

2.2.8.6 Manual Trigger

The Manual Trigger setting can be found under this path: **System> Events> Manual Trigger**.

Using the Manual Trigger setting, the current image(s) or video can be uploaded to the appointed destination, such as an FTP site or an email address. The administrator can specify the actions to be performed when the user switches the Manual Trigger button to ON.

Manual Trigger

The default setting for the Manual Trigger function is <Off>. Enable the function by selecting <On>. After the Manual Trigger function is enabled, click the Manual Trigger button on the Home page to start uploading data. Click again to stop uploading.

Triggered Action (Multi-option)

The administrator can specify alarm actions to be performed at an alarm occurrence.

- **Enable Alarm Output**
  Select the item to enable alarm relay outputs.

- **IR Cut Filter**
  Select the item and the IR cut filter (ICR) of the camera is removed (on) or put in place (off) when alarm input is triggered.

  Note: The IR Function (See section *IR Function*) cannot be set to <Auto> if this triggered action is enabled.

- **Send Message by FTP/E-Mail**
  The administrator can select whether to send an alarm message by FTP and/or email when an alarm is triggered.

- **Upload Image by FTP**
  Select this item and the administrator can assign an FTP site and configure various parameters. When the alarm is triggered, event images are uploaded to the appointed FTP site.

The <Pre-trigger buffer> function allows users to check what caused the trigger. The <Pre-trigger buffer> frame rate can be predetermined. The <Post-trigger buffer> can be used to upload a certain amount of images after the alarm input is triggered.

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

Select the box <Continue image upload> to upload the triggered images for a certain time or to continue uploading until the trigger is off.
Select <Upload for __sec> and then enter the duration in the box.
The images are uploaded to FTP for the set duration when the alarm input is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue the image upload to FTP during the trigger active – that is, until the alarm is released. Set the Image frequency by selecting an upload frame rate. The setting range is from 1 to 15 frames.

NOTE: Make that sure the FTP configuration has been completed. See section *FTP* for further details.

- **Upload Image by E-Mail**
  Select this item and the administrator can assign an email address and configure various parameters. When the alarm is triggered, event images are sent to the appointed email address.

  The <Pre-trigger buffer> function allows users to check what caused the trigger. The <Pre-trigger buffer> frame rate can be predetermined. The <Post-trigger buffer> can be used to upload a certain amount of images after alarm input is triggered.

  NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

Check the box <Continue image upload> to upload the triggered images for a certain time or to continue uploading until the trigger is off. Select <Upload for __sec> and then enter the duration in the box. The images are uploaded by email for the set duration when the alarm input is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue the image upload to email during the trigger active – that is, until the alarm is released. Set the Image frequency by selecting an upload frame rate. The setting range is from 1 to 15 frames

NOTE: Make sure that the SMTP configuration has been completed. See section *Mail* for further details.

- **Send HTTP notification**
  Select this item, and then select the destination HTTP address. Specify the parameters for event notifications by <Alarm> triggered. When an alarm is triggered, the notification can be sent to the specified HTTP server.

  For example, if the custom parameter is set as "action=1&group=2", and the HTTP server name is "http://192.168.0.1/admin.php", the notification will be sent to the HTTP server as "http://192.168.0.1/admin.php? action=1&group=2" when an alarm is triggered.

- **Record Video Clip**
  Select the item and then select a video recording storage type, <SD Card> or <NAS> (Network-Attached Storage). The alarm-triggered recording will be saved to the microSD card or the NAS.

  The <Pre-trigger buffer> recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 seconds. Select <Upload for __ sec> to set the recording duration after an alarm is triggered. The setting range is from 1 to 99999 seconds. Select <Upload during the trigger active> to record the triggered video until the trigger is off.

NOTE: Make sure that local recording (with microSD/SDHC card) or remote recording (with NAS) is activated so that this function can be implemented. See section *Recording* for further details.

File Name

Enter a file name in the File name box. The file name format of the uploaded image can be set in this section. Select one that meets the requirements.

- **Add date/time suffix**
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number

- **Add sequence number suffix (no maximum value)**
  File name: imageXXXXXXX.jpg
  X: Sequence Number

- **Add sequence number suffix (limited value)**
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix will range to the number being set. For example, if the setting is up to “10”, the file name starts at 00, ranges to 10, and then starts all over.

- **Overwrite**
  The original image in the FTP site is overwritten by the new uploaded file with a static filename.

Save

Click <Save> to save all the settings mentioned above.

2.2.8.7 Audio Detection

The Audio Detection setting can be found under this path: **System> Events> Audio Detection**.

The Audio Detection function allows the camera to detect audio and trigger alarms when the audio volume in the detected area reaches/exceeds the defined sensitivity threshold value

Audio Detection

The default setting for the Audio Detection function is <Off>. Enable the function by selecting <On>.

Audio Detection Setting

Users can adjust various Audio Detection parameters here.

- **Detection level [1-100]:**
  Use this item to set the detection level for each sampling volume. The smaller the value, the more sensitive it is. The default level is 10.

- **Time interval (sec) [0-7200]:**
  The value is the interval between each detected audio event. The default interval is 10.

Triggered Action (Multi-option)

The administrator can specify alarm actions to be executed when audio is detected.

- **Enable Alarm Output**
  Select the item and select the predefined type of alarm output to enable alarm relay output when audio is detected.

- **Send Message by FTP/E-Mail**
  The administrator can select whether to send an alarm message by FTP and/or email when an alarm is triggered.

- **Upload Image by FTP**
  Select this item and the administrator can assign an FTP site and configure various parameters. When the alarm is triggered, event images are uploaded to the appointed FTP site.

The <Pre-trigger buffer> function allows users to check what caused the trigger. The <Pre-trigger buffer> frame rate can be predetermined. The <Post-trigger buffer> can be used to upload a certain amount of images after the alarm input is triggered.

NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

Select the box <Continue image upload> to upload the triggered images for a certain time or to continue uploading until the trigger is off.
Select <Upload for __sec> and then enter the duration in the box.
The images are uploaded to FTP for the set duration when the alarm input is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue the image upload to FTP during the trigger active – that is, until the alarm is released. Set the Image frequency by selecting an upload frame rate. The setting range is from 1 to 15 frames.

NOTE: Make that sure the FTP configuration has been completed. See section *FTP* for further details.

- **Upload Image by E-Mail**
  Select this item and the administrator can assign an email address and configure various parameters. When the alarm is triggered, event images are sent to the appointed email address.

  The <Pre-trigger buffer> function allows users to check what caused the trigger. The <Pre-trigger buffer> frame rate can be predetermined. The <Post-trigger buffer> can be used to upload a certain amount of images after alarm input is triggered.

  NOTE: Normally, the setting range of the <Pre-trigger buffer> is 1 to 20. However, the setting range changes accordingly if the frame rate of MJPEG on the <Video Frame Rate> setting page is 6 or smaller.

Check the box <Continue image upload> to upload the triggered images for a certain time or to continue uploading until the trigger is off. Select <Upload for __sec> and then enter the duration in the box. The images are uploaded by email for the set duration when the alarm input is triggered. The setting range is from 1 to 9999 seconds. Select <Upload during the trigger active> to continue the image upload to email during the trigger active – that is, until the alarm is released. Set the Image frequency by selecting an upload frame rate. The setting range is from 1 to 15 frames

NOTE: Make sure that the SMTP configuration has been completed. See section *Mail* for further details.

- **Send HTTP notification**
  Select this item, and then select the destination HTTP address. Specify the parameters for event notifications by <Alarm> triggered. When an alarm is triggered, the notification can be sent to the specified HTTP server.

  For example, if the custom parameter is set as "action=1&group=2", and the HTTP server name is "http://192.168.0.1/admin.php", the notification will be sent to the HTTP server as "http://192.168.0.1/admin.php? action=1&group=2" when an alarm is triggered.

- **Record Video Clip**
  Select the item and then select a video recording storage type, <SD Card> or <NAS> (Network-Attached Storage). The alarm-triggered recording will be saved to the microSD card or the NAS.

  The <Pre-trigger buffer> recording function allows users to check what caused the trigger. The pre-trigger buffer time range is from 1 to 3 seconds. Select <Upload for __ sec> to set the recording duration after an alarm is triggered. The setting range is from 1 to 99999 seconds. Select <Upload during the trigger active> to record the triggered video until the trigger is off.

NOTE: Make sure that local recording (with microSD/SDHC card) or remote recording (with NAS) is activated so that this function can be implemented. See section *Recording* for further details.

File Name

Enter a file name in the File name box. The file name format of the uploaded image can be set in this section. Select one that meets the requirements.

- **Add date/time suffix**
  File name: imageYYMMDD_HHNNSS_XX.jpg
  Y: Year, M: Month, D: Day
  H: Hour, N: Minute, S: Second
  X: Sequence Number

- **Add sequence number suffix (no maximum value)**
  File name: imageXXXXXXX.jpg
  X: Sequence Number

- **Add sequence number suffix (limited value)**
  File Name: imageXX.jpg
  X: Sequence Number

  The file name suffix will range to the number being set. For example, if the setting is up to “10”, the file name starts at 00, ranges to 10, and then starts all over.

- **Overwrite**
  The original image in the FTP site is overwritten by the new uploaded file with a static filename.

Save

Click <Save> to save all the settings mentioned above.

2.2.9 Storage Management (Local Recording)

The Storage Management setting can be found under this path: **System> Storage Management**.

Clicking the <Storage Management> menu, opens a submenu with options including <SD Card> and <Network Share>.

2.2.9.1 SD Card

The SD Card setting can be found under this path: **System> Storage Management> SD Card**.

Users can implement local recording to the microSD/SDHC card up to 64 GB. This page shows the capacity information of the microSD card and a recording list with all the recorded files saved on the memory card. Users can also format the SD card and implement automatic recording cleanup through the setting page.

To implement microSD card recording, go to the <Recording> page (see section *Recording*) for activation.

NOTE: Format the microSD/SDHC card when using it for the first time. Formatting is also required when a memory card already used on one camera is later transferred to another camera with a different software platform.

NOTE: It is not recommended to record with the microSD card for 24/7 continuously, as it may not be able to support long-term continuous data read/write operations. Contact the manufacturer of the microSD card for information regarding the reliability and the life expectancy.

Device information

When users insert the microSD/SDHC card, the card information such as the memory capacity and status are shown in the Device Information section.

When the memory card has been successfully installed, its status is shown in the <Device information> section in the Storage Management page.

Device setting

Click <Format> to format the memory card.

Disk cleanup setting

Users can enable automatic recordings cleanup by specifying the time and storage limits. The setting range of time limits is from 1 to 999 day(s) or 1 to 142 week(s), and the setting range of storage limits is from 1 to 99% full.

Recording List

Each video file on the microSD/SDHC card is listed in the Recording list. The maximum file size is 60 MB (60 MB per file). When the recording mode is set to “Always” (consecutive recording) and microSD/SDHC card recording is allowed to be enabled by events triggered, the system immediately starts recording to the memory card once an event occurs. The camera returns to regular recording mode after event recording.

- **Remove**
  To remove a file, select the file first, and then click <Remove>.

- **Sort**
  Click <Sort> and the files in the Recording list are listed in name and date order.

  NOTE: The capital letter A / M / N / R / T / V appearing in a file name denotes the type of the recording: A stands for Alarm; M stands for Motion; N stands for Network Failure; R stands for Regular Recording, T stands for Tampering, and V stands for Manual Trigger.

- **Download**
  To open/download a video clip, select the file and then click the <download> button below the Recording list. The selected file window pops up. Click the AVI file to directly play the video in the player or download it to a specified location.

2.2.9.2 Network Share (NAS)

The Network Share setting can be found under this path: **System> Storage Management> Network Share**.

Users can store the recorded videos in a network share folder, or NAS (Network-Attached Storage). A NAS device is used for data storage and data sharing via the network. This page displays the capacity information of the network device and a recording list with all the recorded files saved on the network device. Users can also format the NAS and implement automatic recording cleanup through the setting page.

Device information

When a NAS is successfully installed, the device information such as the memory capacity and status is shown in the <Device Information> section.

Storage setting

The administrator can set the camera to send the alarm messages to a specific NAS site when an alarm is triggered. Enter the network device details, which include the host details (the IP of the NAS), the share (the folder name of the NAS), a user name, and a password, in the boxes.

Click <Save> when finished.

Storage Tools

Click <Format> to format the NAS.

Disk cleanup setting

Users can enable automatic recording cleanup by specifying the time and storage limits. The setting range of time limits is from 1 to 999 day(s) or 1 to 142 week(s), and the setting range of storage limits is from 1 to 99% full.

Recording List

Each video file on the Network Share is listed in the Recording list. The maximum file size is 60 MB per file.

When the recording mode is set to <Always> (consecutive recording) and the NAS recording is allowed to be enabled by events triggered, the system immediately starts recording to the NAS, once an event occurs. After the recording of the events is finished, the camera returns to the regular recording mode.

- **Remove**
  To remove a file, select the file and then click <Remove>.

- **Sort**
  Click <Sort> and the files in the Recording list are listed in name and date order.

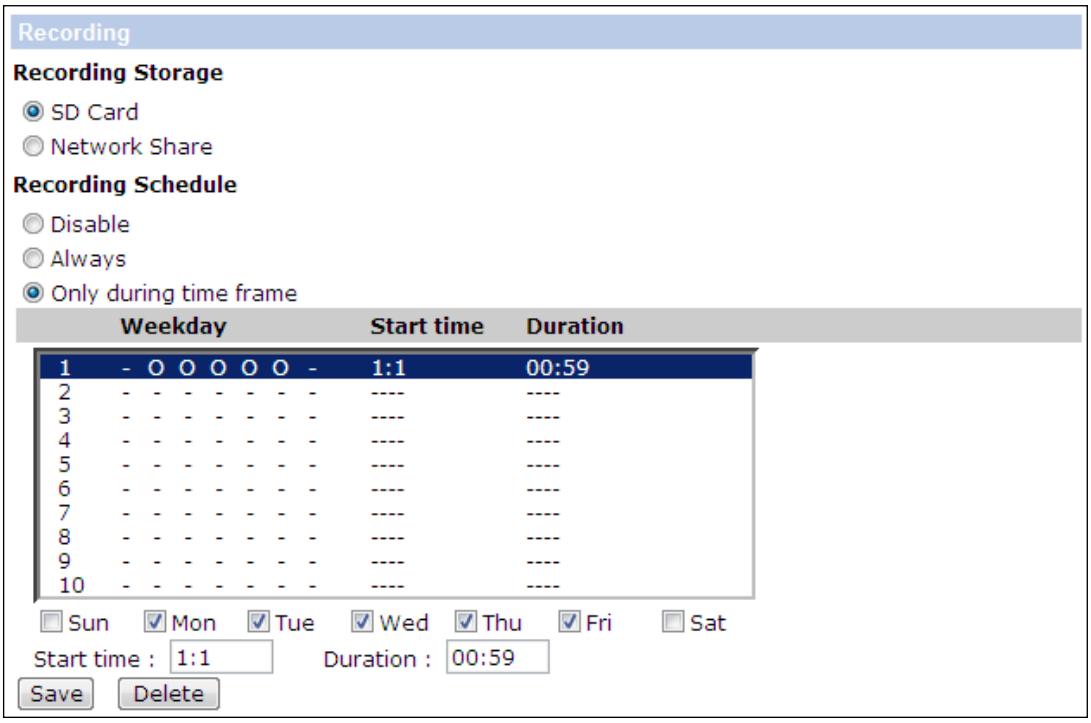
  NOTE: The capital letter A / M / N / R / T / V appearing in a file name denotes the type of the recording: A stands for Alarm; M stands for Motion; N stands for Network Failure; R stands for Regular Recording, T stands for Tampering, and V stands for Manual Trigger.

- **Download**
  To open/download a video clip, select the file and then click the <download> button below the Recording list. The selected file window will pop up. Click the AVI file to directly play the video in the player or download it to a specified location.

2.2.10 Recording (Local Recording)

The Recording setting can be found under this path: **System> Recording**.

In the Recording setting page, user can specify the recording schedule to fit the present surveillance requirement.



Recording Storage

Select a recording storage type, <SD Card> or <Network Share>.

Activating the Recording Schedule

Two schedule modes are offered: <Always> and <Only during time frame>. Users can select <Always> to activate all the time microSD/SDHC card or Network Share recording. Or select a schedule row in the time frame box, select specific weekdays and set up the start time (hour:minute) and time period (hour:minute) to activate the recording at certain time frames. Specify the start time and the duration. The range for the duration is from 0 to 168:59. Click <Save> to save the setup.

Select a recording schedule from the schedule list, and then click <Delete> to delete a recording schedule.

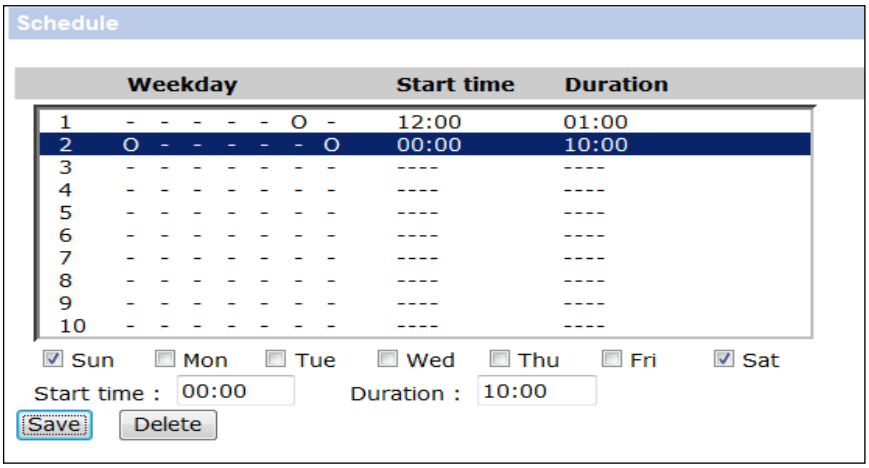
Terminating the Recording Schedule

Select <Disable> to terminate the recording function.

2.2.11 Schedule

The Schedule setting can be found under this path: **System> Schedule**.

This function allows the users to set up schedules for features such as <Alarm Switch>, <Motion Detection>, <Network Failure Detection>, and <Tampering>. The function supports up to 10 sets of time frames in the time frame list.



Setting Schedules

To set a schedule, select a time frame from the time frame list first. Then check the boxes below to choose the specific weekdays. At last, enter the start time (hour:minute) and the duration time (hour:minute) for activation of the schedule triggered features. The setting range for the duration time is from 00:00 to 168:59. Click <Delete> to delete a chosen time frame. Click <Save> to save the setup.

Time Mode

- **Day**
  The camera profile is loaded when the IR cut filter is off.

- **Night**
  The camera profile is loaded when the IR cut filter is on.

- **Time**
  This indicates the start time and the time duration for the schedule.

NOTE: Users *must* select <By schedule> on each feature setting page to enable the schedule function.

2.2.12 File Location (Snapshots and Web Recording)

The File Location setting can be found under this path: **System> File Location**.

Users can specify a storage location for the snapshots and live video recording. The default setting is: C:\. To confirm the setting, click <Save> and all the snapshots and web recording will be saved to the designated location.

NOTE: Make sure that the selected file path contains valid characters such as letters and numbers.

NOTE: Under the Windows 7 (or higher) operating system, to implement the Snapshot and Web Recording function, users must run IE as administrator. To run IE as administrator, right-click the IE browser icon, and then select “Run As Administrator” to launch IE.

2.2.13 View Information

The View Information function can be found under this path: **System> View Information**.

Clicking the <View Information> menu, opens a submenu with options including <Log File>, <User Information>, and <Parameters>.

2.2.13.1 Log File

The Log File function can be found under this path: **System> View Information> Log File**.

Click the Log file option to view the system log file. The content of the file provides useful information about connections after system boot-up.

2.2.13.2 User Information

The User Information function can be found under this path: **System> View Information> User Information**.

The administrator can view each added user's login information and privileges (see section *Security*).

Get User Information

All the users in the network are listed in the <User information> section as in the following example:

User: 4321

It indicates that one user's login username is "User", and the password is "4321".

Get User Privacy

Click <get user privacy> at the bottom of the page, and the administrator can view each user's privileges as in the following example:

User: 1:1:0:1

1:1:0:1= I/O access : Camera control : Talk : Listen (see section *Security*)

This denotes that the user has been granted the privileges of I/O access, Camera control, and Listen.

2.2.13.3 Parameters

The Parameters function can be found under this path: **System> View Information> Parameter**.

Click this item to view the parameter settings of the entire system, such as Camera Settings, Mask Information, and Network Information.

2.2.14 Factory Default

The Factory Default setting can be found under this path: **System> Factory Default**.

Users can follow the instructions on this page to reset the IP camera to the factory-default settings if needed.

Full Restore

Click <Full Restore> to recall the factory-default settings. The system will restart in 30 seconds. The IP address will be restored to default. After the system has restarted, reconnect the camera using the default IP address. The default IP address is **192.168.0.250**.

Partial Restore

Click <Partial Restore> to recall the factory-default settings. The system will restart in 30 seconds. Refresh the browser page after the system has restarted.

NOTE: The IP address will not be restored to default.

Reboot

Click <Reboot> and the system will restart without changing current settings. Refresh the browser page after the system has restarted.

2.2.15 Software Version

The Software Version can be found under this path: **System> Software Version**.

The current software version is displayed in the software version page.

2.2.16 Software Upgrade

The Software Upgrade setting can be found under this path: **System> Software Upgrade**.

NOTE: Make sure that the software upgrade file is available before carrying out the software upgrade.

The procedure of software upgrade is as follows.

Step 1. Click <Browse>, and then locate the upgrade file, for example "uImage_userland".

NOTE: Do not change the upgrade file name, or the system will fail to find the file.

Step 2. Select a file type from the drop-down list. In this case, select "uImage+userland.img"

Step 3. Click <Upgrade>. The system will prepare to start the software upgrade. Subsequently, an upgrade status bar is displayed on the page to show the current upgrade process. After the upgrade process has finished, the viewer returns to the home page.

Step 4. Close the video browser.

Step 5. In the Windows Start menu, click <Control Panel>. Click <Programs and Features>. A window with <Uninstall or change a program> is opened. In the <Name> column, click <TKH Security Viewer>, and then click <Uninstall>. The existing TKH Security Viewer is uninstalled.

Step 6. Reopen your web browser, and then log on to the camera. Allow the automatic download and installation of TKH Security Viewer.

2.2.17 Maintenance

The Maintenance setting can be found under this path: **System> Maintenance**.

Users can export configuration files to a specified location and retrieve data by uploading an existing configuration file to the camera.

Export Files

Users can save the system settings by exporting the configuration file (.bin) to a specified location for future use. Click <Export>, and the information bar prompts you to open or save the configuration file. Click <Save>, and then specify a desired location to save the configuration file to.

Upload Files

To upload a configuration file to the camera, click <Browse> to select the configuration file, and then click <Upload> to upload the file.

2.3 Streaming

On the <**Streaming**> tab, there are submenus including: <Video Format>, <Video Compression>, <Video OCX Protocol>, <Video Frame Rate>, <Video Mask>, and <Audio>.

In the Streaming submenus, the administrator can configure settings related to video resolution, video compression, video protocol, and audio transmission. Details about these settings are specified in the following sections.

2.3.1 Video Format

Video Format setting can be found under this path: **Streaming> Video Format**.

Video Resolution

In the Video Resolution section, the available video resolution formats include the following options:

- H.264 Only
- MJPEG Only
- H.264 + H.264
- H.264 + MJPEG
- H.264 + H.264 + H.264
- H.264 + H.264 + MJPEG
- H.264 + H.264 + H.264 + H.264
- H.264 + H.264 + H.264 + MJPEG

You can set up the video resolution as follows.

Step 1. On the Video Resolution list, select a streaming format combination.

Step 2. Use a Format list to select a resolution.

Step 3. Use the associated Stream list to assign the selected resolution to one of the available streams (for example, H.264-1, etc.).

Step 4. Repeat steps 2 and 3, for the other stream(s), if any.
In this way, you can set up streaming using different resolutions to satisfy different live viewing and recording scenarios.

Step 5. Click <Save> to confirm the setting.

Video Rotate Type

Users can change the video display type if necessary. Selectable video rotation types include Normal, Flip, Mirror, 90 degree clockwise, 180 degree rotate, and 90 degree counterclockwise.

.

- **Flip**
  The image is rotated across the horizontal axis.

- **Mirror**
  The image is rotated across the vertical axis.
- **90 Degree clockwise**
  The image is rotated 90° degrees clockwise.

- **90 Degree counter-/clockwise**
  The image is rotated 90° degrees counterclockwise.

- **180 Degree Rotate**
  The image is rotated 180° degrees.

Click <Save> to confirm the setting.

GOV Settings

Users can set the GOV length to determine the frame structure (I-frames and P-frames) in a video stream to save bandwidth. Less bandwidth is needed if the GOV length is set to a high value. However, the shorter the GOV length the better the video quality is. The setting range is from 1 to 255. The default value for H.264-1 / H.264-2 / H.264-3 / H.264-4 is 60 / 60 / 30 / 30 (NTSC) or 50 / 50 / 25 / 25 (PAL). Click <Save> to confirm the GOV setting.

H.264 Profile

Users can set each H.264 Profile to <Baseline Profile>, <Main Profile> or <High Profile> according to the compression needs. With the same bit rate, the higher the compression ratio, the better the image quality is. The default setting is <Main Profile>.

NOTE: Make sure that the compression ratio you select is supported by the system.

Click <Save> to confirm the setting.

2.3.2 Video Compression

The Video Compression setting can be found under this path: **Streaming> Video Compression**.

This page allows the administrator to adjust the bit rate of MJPEG and H.264-1 / H.264-2 / H.264-3 / H.264-4. Higher values give higher visual quality. Higher bit rates consume more bandwidth, however.

MJPEG Q (Quality) factor

The default setting of MJPEG Q factor is 35; the setting range is from 1 to 70.

H.264-1 / H.264-2 / H.264-3 / H.264-4 bit rate

The default setting of H.264-1 is 4096 kbit/s and for H.264-2 / H.264-3 / H.264-4 is 1024 kbit/s; the setting range for H.264-1 is from 64 to 20480 kbps and for H.264-2 / H.264-3 / H.264-4 is from 64 to 2048 kbit/s.

Display Compression Information

Users can also decide whether to display compression information on the home page.

CBR Mode Setting

The CBR (Constant Bit Rate) mode could be the preferred bit rate mode if the bandwidth available is limited. It is important, however, to take the image quality into account when you choose to use CBR mode.

Click <Save> to confirm the setting.

2.3.3 Video Text Overlay

The camera features programmable on-screen display (OSD) facilities. Date and time information, a subtitle, a text string, and an image (such as a logo) can be displayed as overlays over the camera images.
You can add a text overlay as follows.

Step 1. Select the text overlay type you wish to add.

- *Include date & time*: available options are 'date', 'time', or 'date & time'.
- *Include subtitle:* up to three text boxes can be used.
- *Include text string:* type the text you wish to add.

Step 2. Align the text(s) as necessary and drag the text box(es) to the desired position on the preview.

Step 3. Click Set.

Step 4. In the Text overlay color list, select a font colour.

Step 5. In the Text overlay size list, set the text size to small, medium or large.

Step 6. Click Set.

You can add an image overlay as follows.

Step 1. In the Overlay type section, click Include Image.

Step 2. Drag the image box to the desired position on the preview.

Step 3. Under Image overlay setting, click Browse.
Locate and select an image that meets the following requirements:
Format: 8-bit .bmp, width: a multiple of 32 pixels, height: a multiple of 4 pixels

Step 5. Click Upload.

Step 6. Type a value in the Image transparency box.

Step 6. Click Set.

2.3.4 Video OCX Protocol

The Video OCX Protocol setting can be found under this path: **Streaming> Video OCX Protocol**.

On the Video OCX protocol page, users can select RTP over UDP, RTP over RTSP (TCP), RTSP over HTTP or MJPEG over HTTP for streaming video over the network. In the case of multicast networking, users can select Multicast mode. Click <Save> to confirm the setting.

Video OCX protocol setting options include:

- **RTP over UDP / RTP over RTSP(TCP) / RTSP over HTTP / MJPEG over HTTP**

- **Multicast Mode**
  Enter all required data, including <Multicast H.264-1 / H.264-2 / H.264-3 / H.264-4 / MJPEG Video Address>, <Multicast H.264-1 / H.264-2 / H.264-3 / H.264-4 / MJPEG Video Port>, <Multicast Audio Address>, <Multicast Audio Port> and <Multicast TTL> into each box.

2.3.5 Video Frame Rate

The Video Frame Rate page can be found under this path: **Streaming> Video Frame Rate**.

Video frame rate is for setting the frames per second (fps) if necessary.

MJPEG / H.264-1 / H.264-2 / H.264-3 / H.264-4 Frame Rate
The default setting of the MJPEG / H.264-2 / H.264-3 / H.264-4 frame rate is 30 fps (NTSC) or 25 fps (PAL), and the H.264-1 frame rate is 60 fps (NTSC) or 50 fps (PAL). The setting range is from 1 to 60 (NTSC) or 1 to 50 (PAL). The maximum range of the MJPEG / H.264-1 / H.264-2 / H.264-3 / H.264-4 frame rate changes according to the selected video resolution on the <Video Format> page.

Click <Save> to confirm the setting.

NOTE: Lower frame rates decrease video smoothness.

2.3.6 Video Mask

The Video Mask setting can be found under this path: **Streaming> Video Mask**.

Active Mask Function

- **Add a Mask**
  Select a Video Mask checkbox, and a red frame appears in the Live Video pane on the right side. Use the mouse to adjust the mask's size and place it on the target zone by drag and drop.

  NOTE: It is advised to set a Video Mask to twice the size of the object to be masked.

- **Cancel a Mask**
  Clear the checkbox of the Video Mask that is to be deleted.

Mask Setting

- **Mask color**
  Available Mask colors include black, white, yellow, red, green, blue, cyan, and magenta. Click <Save> to confirm the setting.

2.3.7 Audio (Audio Mode and Bit Rate Settings)

The Audio Mode setting can be found under this path: **Streaming> Audio**.

In the Audio page, the administrator can select the transmission mode and audio bit rate.

Transmission Mode

- **Full-duplex (Talk and Listen simultaneously)**
  In Full-duplex mode, the local and remote sites can communicate with each other simultaneously – that is, both sites can speak and be heard at the same time.

- **Half-duplex (Talk or Listen, not at the same time)**
  In Half-duplex mode, the local/remote site can only talk or listen to the other site at a time.

- **Simplex (Talk only)**
  In Talk only Simplex mode, the local/remote site can only talk to the other site.

- **Simplex (Listen only)**
  In Listen only Simplex mode, the local/remote site can only listen to the other site.

- **Disable**
  Select this option to turn off the audio transmission function.

Server Gain Setting

Set the audio input / output gain levels for sound amplification. The audio input gain value is adjustable from 1 to 10. The audio output gain value is adjustable from 1 to 6. The sound is turned off if the audio gain is set to “Mute”.

Bit Rate

Selectable audio transmission bit rates include 16 kbps (G.726), 24 kbps (G.726), 32 kbps (G.726), 40 kbps (G.726), uLAW (G.711) and ALAW (G.711). Both uLAW and ALAW signify 64 kbps but in different compression formats. A higher bit rate gives better audio quality but consumes more bandwidth. Click <Save> to confirm the setting.

Recording to Storage

Select <Enable> from the drop-down list to enable recording audio with video to the SD card or NAS.

NOTE: If the chosen bit rate is not compatible with the player, there will only be noise instead of audio during playback.

2.4 Camera

The submenus on the <**Camera**> tab include: <Exposure>, <White Balance>, <Picture Adjustment>, <Backlight>, <IR Function>, <WDR Function>, <Noise Reduction>, <Fisheye Setting> and <TV System>.

2.4.1 Exposure

The Exposure setting can be found under this path: **Camera> Exposure**.

Exposure is the amount of light received by the image sensor. It is determined by the width of lens diaphragm opening, the shutter speed and other exposure parameters. With these items, users can define how the Auto Exposure function works. Users can select one of the exposure modes according to the operating environment. Click <√> to confirm the new setting.

Each exposure mode is specified as follows.

Auto Mode

- **Max Gain**
  Maximum Gain can be set to reduce image noise. The Max Gain range is 1dB to 3dB, or select <Off> to disable the function. The default setting is 3dB.

- **Auto Shutter Mode**
  In this mode, the camera automatically adjusts the shutter speed according to the light intensity. The minimum shutter speed range is configurable from 1/500 to 1 sec. (NTSC) or 1/425 to 1/1.5 sec. (PAL).

Manual Mode

With this mode, users can select the suitable shutter speed and gain value according to the environmental illumination. The shutter speed range is from 1/10000 to 1 sec. (NTSC) or from 1/10000 to 1/1.5 sec. (PAL). The gain value range is from 1dB to 9dB, or select <Off> to disable the function.

2.4.2 White Balance

The White Balance setting can be found under this path: **Camera> White Balance**.

A camera needs to find a reference color temperature, which is a way of measuring the quality of a light source, to calculate all the other colors. The unit for measuring this ratio is in degree Kelvin (K). Users can select one of the White Balance Control modes according to the operating environment. The following table shows the color temperature of some light sources for reference. Click <√> to confirm the new setting.

Light Sources	Color Temperature in K
Cloudy Sky	6,000 to 8,000
Noon Sun and Clear Sky	6,500
Household Lighting	2,500 to 3,000
75-watt Bulb	2,820
Candle Flame	1,200 to 1,500

Auto Mode (Auto White Balance)

The Auto White Balance mode is suitable for environments with a light source which has a color temperature ranging roughly from 2700K to 7800K.

ATW Mode (Auto Tracking White Balance)

With the Auto Tracking White Balance function, the white balance in a scene is automatically adjusted while the color temperature is changing. The ATW Mode is suitable for environments with a light source which has a color temperature ranging roughly from 2500K to 10000K.

One Push

With the One Push function, the white balance is adjusted and fixed according to the scene the camera sees at the moment. This function is best for situations with minimal scene changes and continuous lighting. The function is suitable for light sources with any kind of color temperature. Follow the steps below to set the white balance.

- Point the camera to the monitoring area.
- Select <One Push> in the White Balance setting menu and click <√>.
- Click the  button to adjust the color tone of the live images.

NOTE: In this mode, the value of white balance does not change as the scene or the light source varies. Therefore, users might have to re-adjust the white balance by clicking the  button again when needed.

Manual Mode

In this mode, users can manually adjust the White Balance value. Enter a number between 0 to 127 for “Rgain/Bgain” to adjust the red/blue illuminant on the Live Video Pane. The following describes several situations that might occur during manual White Balance adjustment.

- The video image turns reddish (as in the left picture below).
  The higher the Rgain value, the redder the image is. To solve the problem, reduce the Rgain value, and the video image turns less reddish.


Reddish Image


Corrected White Balance

- The video image turns greenish (as in the left picture below).
  The lower the Rgain value, the greener the image is. To solve the problem, Increase the Rgain value, and the video image turns less greenish.


Greenish Image


Corrected White Balance

- The video image turns bluish (as in the left picture below).
  The higher the Bgain value, the bluer the image is. To solve the problem, reduce the Bgain value, and the video image turns less bluish.


Bluish Image


Corrected White Balance

- The video image turns yellowish (as in the left picture below).
  The lower the Bgain value, the yellower the image is. To solve the problem, Increase the Bgain value, and the video image turns less yellowish.


Yellowish Image


Corrected White Balance

The following image displays the general color shifts of the scene when different Rgain/Bgain combinations are applied.

2.4.3 Picture Adjustment

The Picture Adjustment setting can be found under this path: **Camera> Picture Adjustment**.

Brightness

The brightness level of the images is adjustable from -12 to +13. Click <√> to confirm the new setting.

Sharpness

The sharpness level of the images is adjustable from +0 to +15. The edge of the objects is enhanced as the sharpness level increases. Click <√> to confirm the new setting.

Contrast

The contrast level of the images is adjustable from -6 to +19. Click <√> to confirm the new setting.

Saturation

The saturation level of the images is adjustable from -6 to +19. Click <√> to confirm the new setting.

Hue

The hue level of the images is adjustable from -12 to +13. Click <√> to confirm the new setting.

2.4.4 IR Function

The IR Function setting can be found under this path: **Camera> IR Function**.

Day/Night Function

With this item, users can define the action of the IR cut filter. See the descriptions of each option below to select a suitable mode. Click <√> to confirm the new setting.

- **Auto Mode**
  With this mode, the camera decides the occasion to remove the IR cut filter.

- **Night Mode**
  Use this mode when the environment light level is low. The IR cut filter is removed to allow the camera to deliver clear images in black and white.

- **Day Mode**
  Select this mode to turn on the IR cut filter. The IR cut filter can filter out the IR light and allows the camera to deliver high quality images in color.

- **Light Sensor Mode**
  The IR LED lights are turned on/off depending on the light sensor.

- **Light On Mode**
  In this mode, the IR LED lights are always on.

- **Light Off Mode**
  In this mode, the IR LED lights are always off.

- **Smart Mode**
  With Smart mode, the camera decides the occasion to remove the IR cut filter. The Smart mode mechanism can judge whether the main light source is from IR illumination or not. If the main light source is from IR illumination, the IR cut filter is kept opened (i.e. monochrome/night mode).

Day/Night Threshold

Use this item to define when the camera should switch from day mode to night mode or vice versa. The camera detects the ambient brightness level. The threshold values indicate the light levels. Once the light level reaches the set threshold, this is detected by the camera and it will automatically switch to Day/Night Mode. The light levels range from 0 to 10, (darker = 0; brighter = 10).

2.4.5 Noise Reduction

The Noise Reduction setting can be found under this path: **Camera> Noise Reduction**.

The camera provides multiple <Noise Reduction> options for delivering optimised image quality especially in extra low-light conditions.

3DNR

3DNR (3D Noise Reduction) delivers optimised image quality especially in extra low-light conditions. Different levels of 3DNR are provided, including Low, Mid and High. The higher level of 3DNR generates relatively enhanced noise reduction.

2DNR

2DNR (2D Noise Reduction) delivers clear images without motion blurs in extra low-light conditions.

ColorNR

In a dark or insufficient light environment, with the camera in color mode, ColorNR (Color Noise Reduction) can eliminate color noise.

Three levels of ColorNR, including Low, Mid and High, are provided. The higher level of ColorNR generates relatively enhanced noise reduction. Click <√> to confirm the new setting.

2.4.6 Profile

The Camera Profile setting can be found under this path: Camera > Profile. Camera Profile allows users to set up the desired image parameters for specific environments with different time schedules. Users can set up up to 10 sets of camera parameter configuration on the Camera tab. To enable this function, users must set up the schedules in advance. See section *Schedule* for further details of schedule setup. Then, follow the steps below to set up a camera profile

Camera Profile Setup

Step 1. On the Camera tab, set up the camera parameters, such as White Balance, Picture Adjustment, etc., excluding TV System.

Step 2. To set up a profile, click the Profile option.

Step 3. Select a number from the Num list and type a name for the profile in the Name box.

Step 4. Click the button below the Name box.
The camera configuration is saved and applied to the profile. A camera profile is created and saved.

Step 5. Select a profile from the Num list.

Step 6. Select the By schedule box and then select the desired schedule(s) from the Schedule list.
Multiple schedules can be applied to one profile.

Step 7. Click the button below <By schedule>.

Step 8. If required, repeat steps 3 – 7 to set additional profiles.
The camera will now automatically switch profiles according to the schedule.

Alternatively, you can manually select a number from the Num list and then click the button. The camera will load and apply the selected profile settings.

NOTE: If you wish to set the camera parameters to the factory default settings, select <Normal> from the Num list. The camera then loads the default values.

NOTE: You must set the camera parameters of the last profile as the default setting. Thus, if there are gaps among the schedules, the camera will apply the setting of the last profile

2.4.7 Backlight

The Backlight setting can be found under this path: **Camera> Backlight**.

The Backlight Compensation function prevents the centre object from being too dark in surroundings where there is excessive light behind the centre object.

Click <√> to confirm the new setting.

2.4.8 Digital Zoom

If digital zoom is enabled, users can rotate the mouse wheel in full screen mode to zoom in and out. Digital zoom is adjustable from x2 to x10.

NOTE: Digital zoom is available in Backend Software Dewarping mode only.

2.4.9 WDR Function

The WDR Function setting can be found under this path: **Camera> WDR Function**.

The Wide Dynamic Range (WDR) function solves high contrast or changing light issues so that video display is enhanced. Available levels for WDR include Low, Mid, and Hi. A higher level of WDR gives wider dynamic range, so that the camera can catch a greater scale of brightness. Click <√> to confirm the new setting.

2.4.10 Fisheye Setting

The Fisheye Correction setting can be found under this path: **Camera> Fisheye Setting**.

On this page, users can choose a dewarping method for correcting the fisheye source images, and select the camera's installation method to view the dewarped images with the correct viewing modes. See the following subsections *Fisheye Dewarping Type* and *Installation* for more details.

After a suitable dewarping method and the correct installation method are selected, users can view the dewarped images from the camera's web browser configuration interface. Click the Fisheye Image Adjustment buttons on the home page and view the dewarped images in the preferred viewing mode. Alternatively, users can view the dewarped images from a backend device or backend software that has dewarping function. See its User Manual for more details.

NOTE: The Fisheye Image Adjustment buttons are different according to the dewarping method and installation method selected on this page. See the tables in subsection *Fisheye Image Adjustment* under section *Function Items on Home Page* for the supported buttons.
Streaming 6 Mpixel is only available in back end dewarping mode.
In front end dewarping mode, the maximum stream resolution is 4 Mpixel. Digital Zoom is only available in Back End Software Dewarping mode.

Fisheye Dewarping Type

With this item, users can choose a method to dewarp the fisheye source images. The options are <Front End Correction> and <Back End Correction>. See below for more details. After a dewarping method is selected, click <Save> to confirm the setting.

- **Front End Camera Dewarping**
  With Front End Camera Dewarping, the fisheye source images are corrected by the camera itself. Having the camera dewarp images can reduce network usage and image processing load of the backend device. It also allows the camera to record or take snapshots of the dewarped images.

With this method, when viewing the dewarped images from the camera's web browser configuration interface, the video format needs to be set to the second stream. See the following instructions to view the dewarped images.

- In the <Installation> section, select the camera's installation method, and then click <Save>. For details, see subsection *Installation* below.
- On the Home page, set the <Video format> under the live video window to H.264-2 or MJPEG.
- The Fisheye Image Adjustment buttons appear on the Home page and in the <Installation> section on the <Fisheye Setting> page.
- Users can view the dewarped images on the Home page or on the <Fisheye Setting> page. Click the buttons to view the dewarped images in the preferred viewing mode.

Note that besides viewing them in a web browser, dewarped images can also be streamed, so that you can view them in a video player application, for example.

- **Back End Software Dewarping**
  Back End Software Dewarping is a dewarping method that has the fisheye source images corrected by a backend device or backend software with dewarping function. Using this method to dewarp can correct high-resolution images and deliver clear dewarped images.

  With this method, users can also view the dewarped images from the camera's web browser configuration interface. The video format can be set to any available stream. The fisheye source images are dewarped by the Viewer and displayed on the Home page. However, users can only record video or take snapshots of the fisheye source images delivered from the camera.

Installation

With this item, users can select the camera's installation method, so the dewarped images can be viewed with the correct viewing modes. Select a method from the drop-down list according to the location where the camera is installed. Choose <Ceiling Mount> if the camera is mounted on a ceiling, or select <Wall Mount> if the camera is mounted on a wall.

Refresh Speed

With this item, users can adjust the speed of the virtual PTZ. The refresh speed options are 5, 10, 15, and 20. The larger the value, the faster the pan tilt movement is.

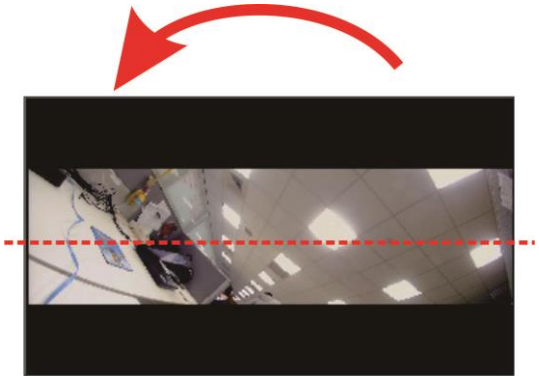
NOTE: This item is only available when <Front End Camera Dewarping> is selected under <Fisheye Dewarping Type>.

Horizontal Calibration

With this item, users can calibrate images counterclockwise/clockwise.

NOTE: This item is only available when <Back End Software Dewarping> is selected under <Fisheye Dewarping Type> and <Wall Mount> is selected under <Installation>.

- **Counterclockwise**
  Users can click on the <1> or <10> button to calibrate the image one degree or ten degrees counterclockwise.



- **Clockwise**
  Users can click on the <1> or <10> button to calibrate the image one degree or ten degrees clockwise.

2.4.11 TV System

The TV System setting can be found under this path: **Camera> TV System**.

Select the video format that matches the present TV system. Click <√> to confirm the new setting.

2.5 Logout

Click the <**Logout**> tab at the top of the page and the login window pops up. This enables a login with a different user name.

Appendix A: Install UPnP Components

Follow the instructions below to install UPnP components on Windows 7 (and higher).

Step1: Open the <Start Menu>, click <Control Panel>, and then click <Network and Sharing Center>.

Step 2: In the left pane, click <Change advanced sharing settings>.

Step 3: Select the appropriate network type.

Step 4: In the Network Discovery section, select the option <Turn on network discovery>.

Step 5: Click <Save changes>.

Appendix B: IP Addresses from Decimal to Binary

Follow the example below to convert IP addresses to binary numbers. Use the calculator on the computer for conversion. The calculator can be found under this path: **Start> All Programs> Accessories> Calculator**. For Windows 7 (or higher), click <View> on the calculator and click <Programmer>. Then follow the steps in the following example to convert the IP addresses.

The example below shows how to convert 192.168.2.81 to binary numbers.

Step 1: On the left of the calculator, select <Dec>. Then enter the first decimal number of the IP address, “192”. Select <Bin> and the number is converted to a binary number. Repeat the same procedure with the rest of decimal numbers. Remember to select <Dec> before entering the next decimal number. Otherwise, a decimal number cannot be entered. The table below shows the binary number for each decimal number.

Decimal Numbers	Binary Numbers
192	11000000
168	10101000
2	10
81	1010001

Step 2: Each binary number should have eight digits. If a binary number does not have eight digits, add 0 in front of it until it does. The binary number of each decimal number should be as follows.

Decimal Numbers	Binary Numbers
192	11000000
168	10101000
2	00000010
81	01010001

Step 3: Therefore, the binary format of IP address 192.168.2.81 is 11000000.10101000.00000010.01010001.