



User Manual

Full HD Day & Night Network Camera

DCS-7110

Preface

D-Link reserves the right to revise this publication and to make changes in the content hereof without obligation to notify any person or organization of such revisions or changes.

Manual Revisions

Revision	Date	Description
2.0	November 25, 2011	DCS-7110 Revision A2 with firmware version 1.10
2.01	March 5, 2012	DCS-7110 Revision A2 with firmware version 1.20
2.10	July 16, 2012	DCS-7110 Revision A3 with firmware version 1.20
3.00	November 26, 2013	DCS-7110 Revision B1 with firmware version 3.00

Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link Corporation or its subsidiaries in the United States or other countries. All other company or product names mentioned herein are trademarks or registered trademarks of their respective companies.

Copyright © 2013 by D-Link Systems, Inc.

All rights reserved. This publication may not be reproduced, in whole or in part, without prior expressed written permission from D-Link Systems, Inc.

Table of Contents

Product Overview	5	Video	33
Package Contents.....	5	Video Settings.....	33
System Requirements.....	6	Image Settings.....	36
Introduction	7	Day and Night Settings.....	38
Features.....	8	Network.....	39
Hardware Overview.....	9	IP Settings.....	39
Front Panel	9	Port and Access Name Settings.....	42
Cable Connectors	10	Dynamic DNS	45
Rear panel	11	HTTPS.....	46
Installation	12	Access List.....	48
Hardware Installation.....	12	Advanced Settings	50
Mounting the Camera.....	12	Event Management	54
Deploying the Camera.....	13	Motion Detection	54
Cable Connections.....	14	Tamper Detection.....	55
Software Installation	16	DI and DO	56
Setup Wizard	16	Event Settings	57
Web-based Configuration Utility.....	21	Recording	63
D-ViewCam Setup Wizard.....	23	Recording Settings.....	63
Configuration	25	PTZ Control	65
Live Video	25	Digital PTZ.....	65
Client Setup.....	29	User Customization.....	66
Setup.....	30	Live Video Page Configuration.....	66
Basic Setup.....	30	HTML Code Examples	67
Advanced Setup.....	31	System	68
System Overview	32	User Settings	68
		Device Settings.....	69

Time and Date.....	70
Maintenance.....	71
Parameter List	73
Logs	74
Appendix A - Technical Specifications.....	75
Technical Specifications.....	75

Package Contents



Network Camera



Mounting Bracket



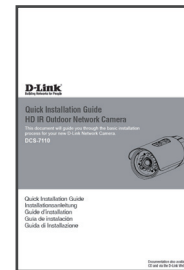
User Manual and Software on CD-ROM



Power Adapter



Screw



Quick Install Guide



CAT5 Ethernet Cable

If any of the above items are missing, please contact your reseller.

System Requirements

- Operating System: Microsoft Windows®, 2000, XP, Vista, 7
- Memory : At least 256MB of memory (512MB recommended)
- Web Browser: Internet Explorer 6.x or higher
- VGA card resolution: SVGA or XGA (1024x768 or above)
- CPU: 1.7GHz or above (2.8GHz plus processor with 512MB memory and a 32MB video card is required for multiple camera viewing and recording in IP surveillance program)
- An available Ethernet connection

Introduction

D-Link DCS-7110 is an all-in-one, outdoor network camera equipped with industry-leading Full HD megapixel resolution and H.264 compression. The DCS-7110 connects to a network to provide high-quality live video over the Internet. This camera is capable of capturing video in both dark and light environments thanks to its built-in IR LEDs and IR-cut removable (ICR) filter. The ICR filter can be manually applied via the web, or set to automatically adjust based on lightning conditions. This feature allows the camera to capture crisp color images during the daytime and detailed grayscale images at night or in or low-light conditions.

The included D-Link D-ViewCam™ is sophisticated software which allows users to manage up to 32 network cameras, set e-mail alert notifications, create recording schedules, and use motion detection to record directly to a hard drive. D-ViewCam™ also allows users to upload a floor plan to create a realistic layout of the premises where cameras are located, further simplifying the management process.

Features

Flexible Connectivity

The DCS-7110 includes input and output ports for connectivity to external devices such as IR sensors, switches, and alarm relays. The DCS-7110 also incorporates Power over Ethernet (PoE), allowing it to be easily installed in a variety of locations without the need for supplemental power cabling.

High-Quality Video at HD Resolution

The DCS-7110 provides real-time video feeds at up to 15fps with Full HD resolution and 30 fps with HD resolution. H.264 encoding ensures that images remain crisp, clear, and vivid without taking up too much network bandwidth.

Weather-proof with Tamper Detection

Designed to be mounted outdoors, the DCS-7110 includes an IP66 certified enclosure which protects against the elements. Anti-tamper features make this camera suitable for tamper-prone locations such as transportation hubs, schools, or correctional facilities. The electronic tamper detection system can sense whenever the camera has been redirected, de-focused, blocked, or spray-painted, and respond promptly with a visible or audible alarm.

Advanced Web User Interface

The DCS-7110 features D-Link's latest-generation graphical user interface. This freshly-designed web interface features a clean, compact, and professional home screen which dramatically increases usability. Menu navigation is simplified thanks to a tree view which logically groups functions, helping users to quickly find what they need. Likewise, intuitive graphic icons reduce the amount text and clutter within the browser window. New users will appreciate the convenient contextual help which offers an easy way to find assistance with camera management tasks.

Hardware Overview

Front Panel



Cable Connectors



DC Power

Connects to the 12 V DC power adapter to power the camera

AC

24 V AC power wiring can be connected to the AC connectors to power the camera.

Ethernet (PoE)

RJ-45 connector is for Ethernet and can also be used to power the camera using PoE

DI/DO Connectors

DI/DO connectors provide a physical interface to send and receive digital signals to and from a variety of external devices

Rear panel



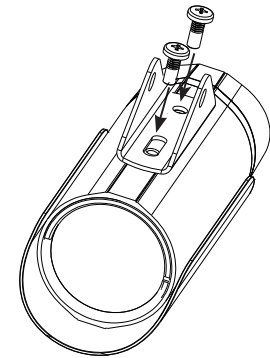
Rest Button

Removing the weatherproof cover, use a paperclip or similar tool to press and hold the recessed button for 10 seconds to reset the camera back to the factory default settings

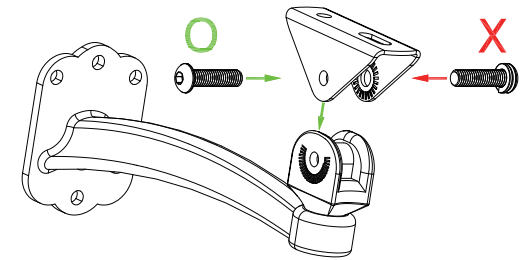
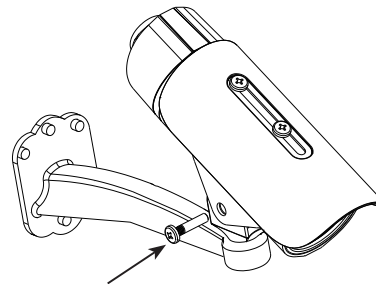
Hardware Installation

Mounting the Camera

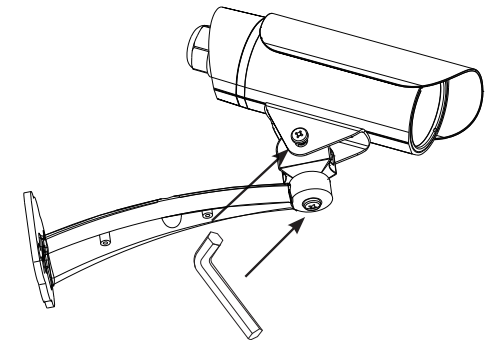
Step1: Using the two screws provided attach camera shoe to the underside of the camera.



Step2: Using the bolt provided attach camera shoe to the mounting bracket and adjust the vertical orientation of the camera.



Step3: Using the Allen Wrench provided, loosen the bolts and adjust the vertical / horizontal orientation of the camera to desired field of view. Firmly tighten the adjustment bolts and lock it into the place.

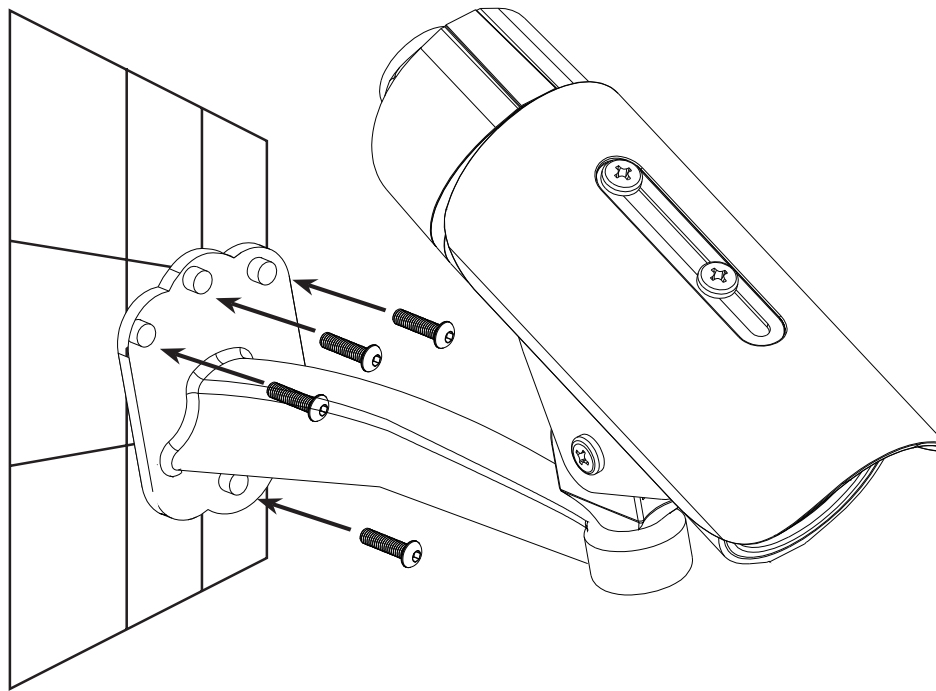


Deploying the Camera

Step1: Locate an area on the wall which is capable of supporting the weight of the camera.

Step2: Use a drill bit to make holes. Insert wall anchors and affix the mounting bracket using the screws provided.

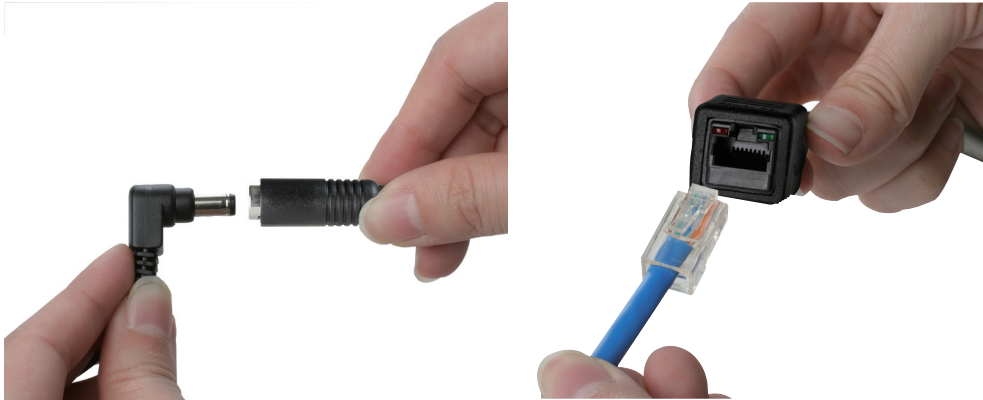
Step3: The camera cables can be installed through a separate large hole drilled in the wall, or using an external cable conduit.



Cable Connections

Basic Connection (without PoE)

1. Connect the camera to your switch or router via Ethernet cable.
2. Connect the power cable from the camera to the supplied power adapter.
3. Connect the supplied power adapter to a power outlet.



Connection Using a PoE Switch

If using a PoE switch or router, connect the network camera via Ethernet cable. PoE will transmit both power and data over a single cable.



Note: Once power has been established, the LED will turn red. When the device has obtained an IP address and is accessible, the LED will turn green.

Note: To prevent the camera's wire connectors from being damaged by water or other elements:

1. When connecting the camera, the unsheathed part of the wire connectors must either be sealed or enclosed in a junction box.
2. The unsheathed part of the wire connectors should be positioned at a downward-facing angle when they extend out of the rear of the camera, not upward.



The unsheathed part of the wire connectors must either be sealed or enclosed in a junction box.

Software Installation

Setup Wizard

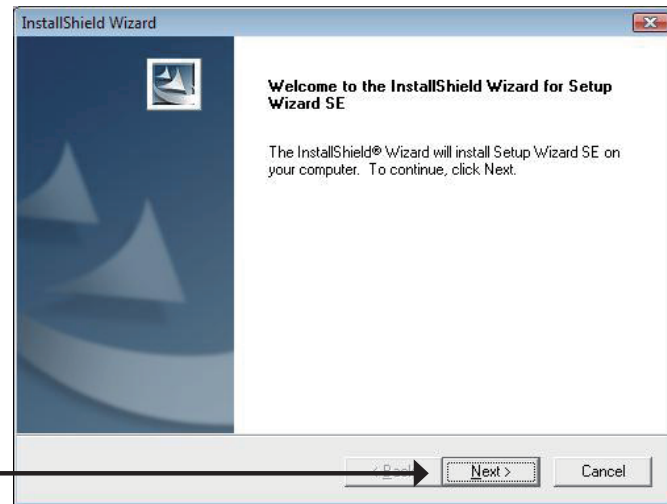
Insert the DCS-7110 CD into your computer's CD-ROM drive to begin the installation. If the Autorun function on your computer is disabled, or if the D-Link Launcher fails to start automatically, click **Start > Run**. Type **D:\autorun.exe**, where D: represents the drive letter of your CD-ROM drive.

Click **Setup Wizard** to begin the installation.

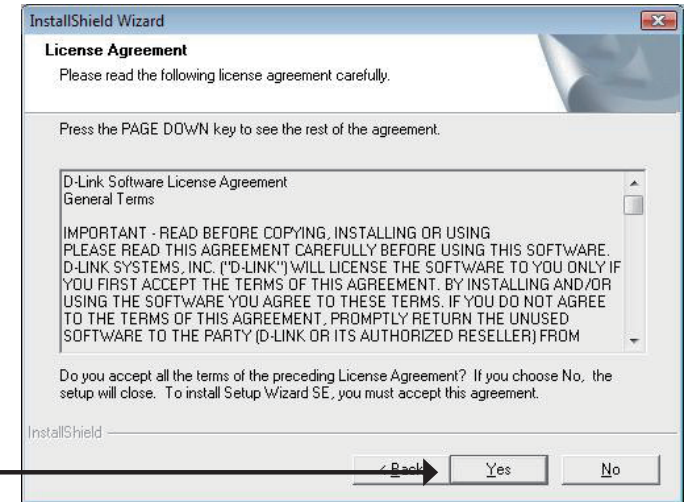


After clicking Setup Wizard, the window on the right will open.

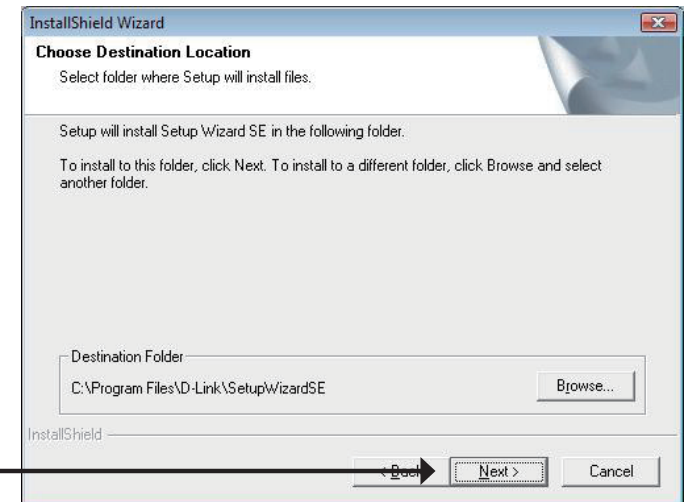
Click **Next** to continue.



Click **Yes** to accept the License Agreement.

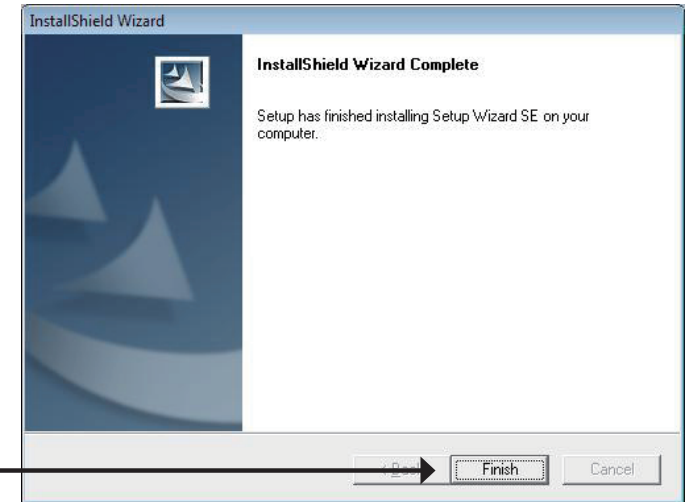


To start the installation process, click **Next**.



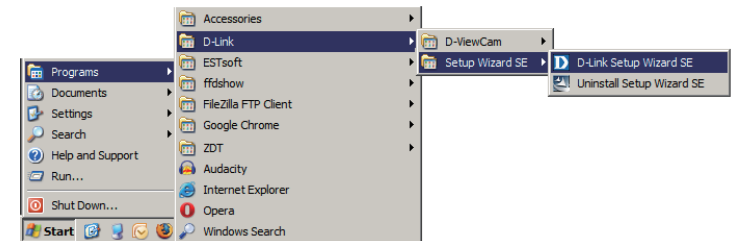
Note: The installation may take several minutes to finish.

Click **Finish** to complete the installation.



Click on the **D-Link Setup Wizard SE** icon that was created in your Windows Start menu.

Start > D-Link > Setup Wizard SE



Installation

The Setup Wizard will appear and display the MAC address and IP address of your camera(s). If you have a DHCP server on your network, a valid IP Address will be displayed. If your network does not use a DHCP server, the network camera's default static IP address **192.168.0.20** will be displayed.

Click the **Wizard** button to continue.



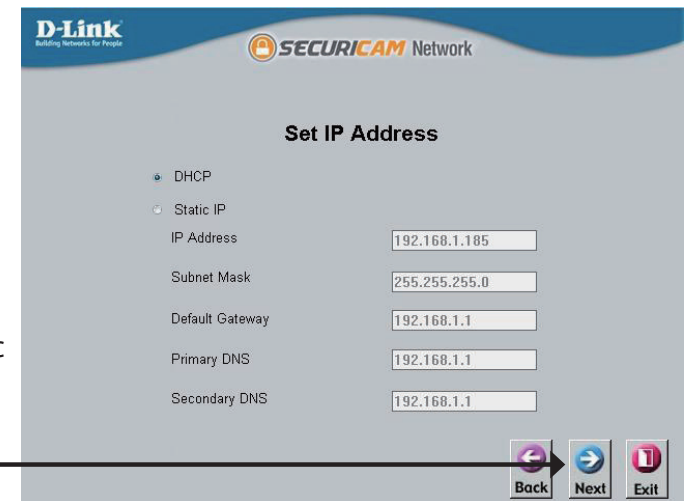
Enter the Admin ID and password. When logging in for the first time, the default Admin ID is **admin** with the password left blank.

Click **Next**, to proceed to the next page.



Select DHCP if your camera obtains an IP address automatically when it boots up. Select static IP if the camera will use the same IP address each time it is started.

Click **Next**, to proceed to the next page.



D-Link Building Networks for People

SECURICAM Network

Set IP Address

DHCP

Static IP

IP Address

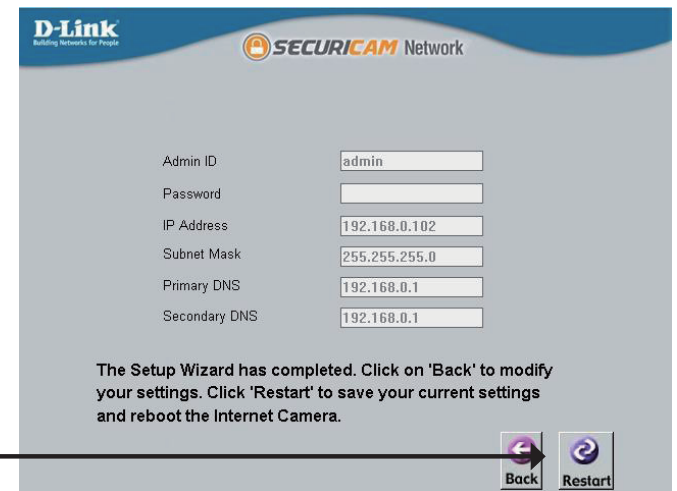
Subnet Mask

Default Gateway

Primary DNS

Secondary DNS

Take a moment to confirm your settings and click **Restart**.



D-Link Building Networks for People

SECURICAM Network

Admin ID

Password

IP Address

Subnet Mask

Primary DNS

Secondary DNS

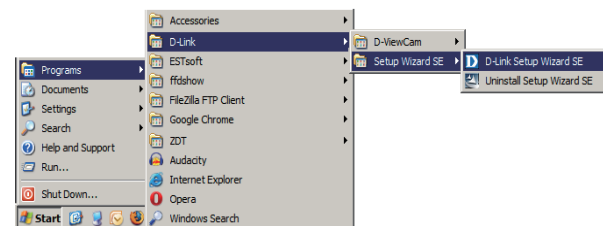
The Setup Wizard has completed. Click on 'Back' to modify your settings. Click 'Restart' to save your current settings and reboot the Internet Camera.

Web-based Configuration Utility

This section explains how to configure your new D-Link Network Camera using the Web-based Configuration Utility.

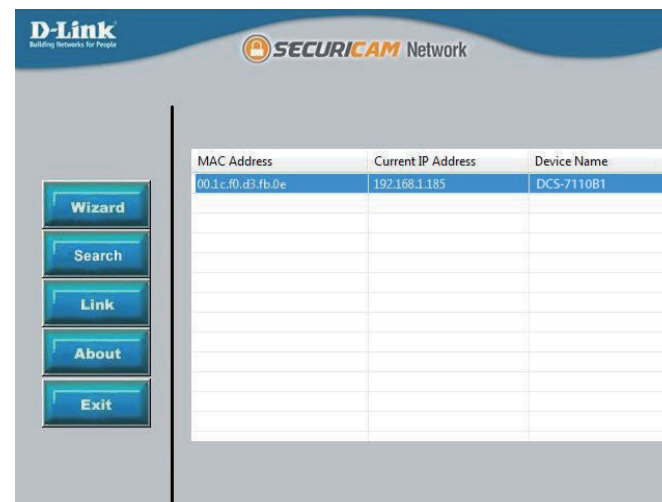
Click on the **D-Link Setup Wizard SE** icon that was created in your Windows Start menu.

Start > D-Link > Setup Wizard SE

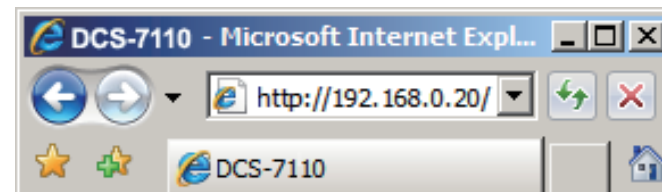


Select the camera and click the button labeled **"Link"** to access the web configuration.

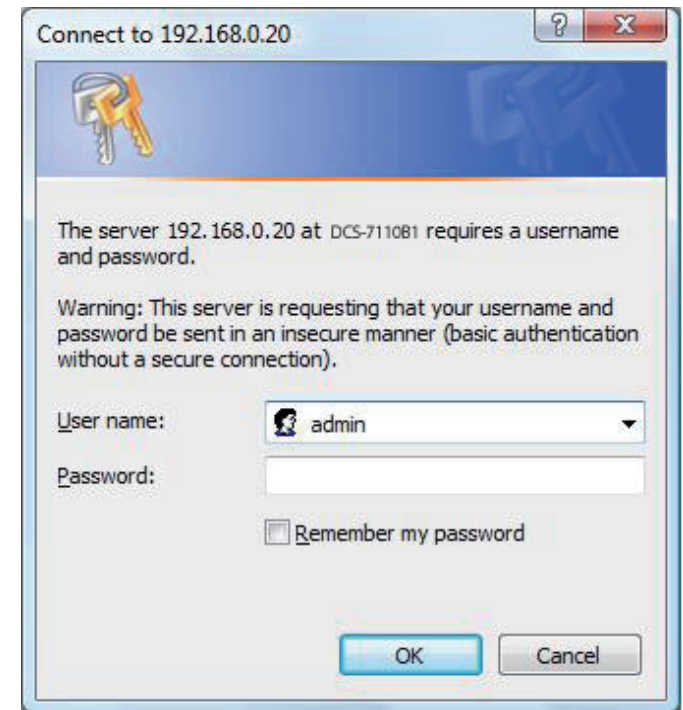
The Setup Wizard will automatically open your web browser to the IP address of the camera.



Alternatively, you may manually open a browser and enter the IP address of the camera: **192.168.0.20**



Enter **admin** as the default username and leave the password blank. Click **OK** to continue.



This section shows your camera's live video. You can select your video profile and view or operate the camera. For additional information about web configuration, please refer to the user manual included on the CD-ROM or the D-Link website.



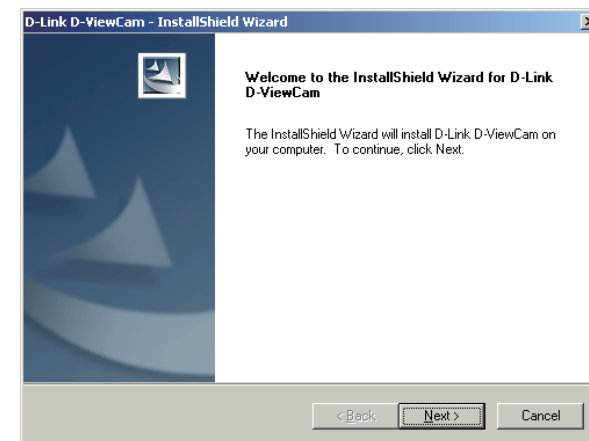
D-ViewCam Setup Wizard

D-ViewCam software is included for the administrator to manage multiple D-Link IP cameras remotely. You may use the software to configure all the advanced settings for your cameras. D-ViewCam is a comprehensive management tool for IP surveillance.

Insert the CD-ROM into the CD-ROM drive. Click "Install D-ViewCam Software" from menu, and select "D-ViewCam" to install the VMS software.



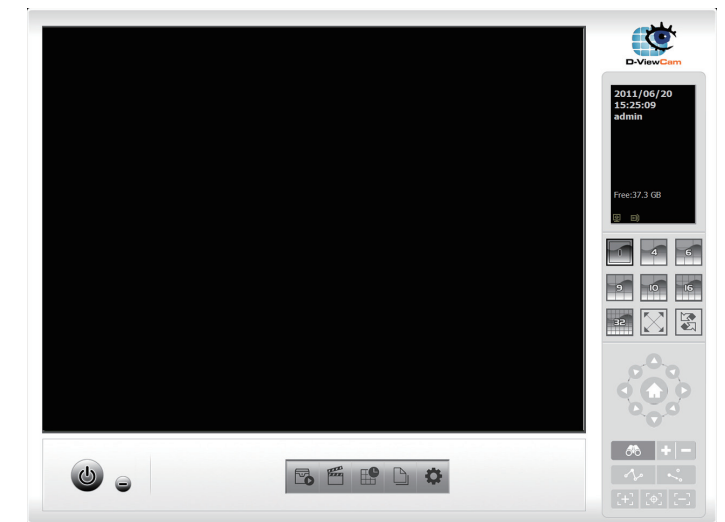
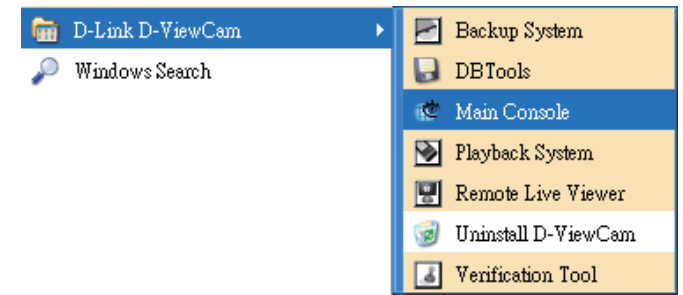
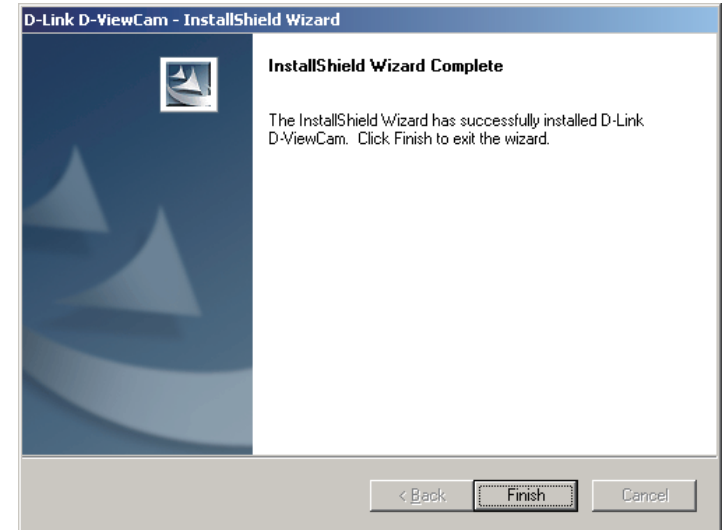
Follow the Installation Wizard to install D-ViewCam.



Click **Finish** to complete the installation.

To start D-ViewCam, select **Start > All Programs > D-Link D-ViewCam > Main Console**.









For more detail operation of using D-ViewCam software, please refer to D-ViewCam Manual.











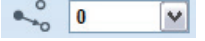




Live Video

When you connect to the camera's web interface you will see the following page. This is the Live Video page which will allow you to view the camera's video feed and control basic camera functions using the icons on the screen. Please refer to the tables on the following pages for detailed information about the icons on this screen.



	<p>Click this logo to visit the D-Link website. The logos and website can be customized to fit your needs. For more information, please refer to User Customization on page 66.</p>
	
 <p>Client Settings</p>	<p>Setup the stream transmission mode and saving options on the local computer.</p>
 <p>Language</p>	<p>Select this option to adjust the language settings.</p>
 <p>Setup</p>	<p>Click on the setup icon on the main page to enter the camera setting pages. Note that only Administrators can access the setup page. To simplify the setting procedure, two types of user interfaces are available: Advanced Setup for professional users and Basic Setup for entry-level users.</p>
 <p>Digital Output</p>	<p>Click this button to turn the digital output device on or off.</p>
 <p>Video Stream</p>	<p>This camera supports multiple streams (stream 1 ~ 4) simultaneously. You may select one for live viewing.</p>
 <p>Global View</p>	<p>Click on this item to display the Global View window. The Global View window contains a full view image (the largest frame size of the captured video) and a floating frame (the viewing region of the current video stream). The floating frame allows users to control the e-PTZ function (Electronic Pan/Tilt/Zoom). For more information about e-PTZ operation, please refer to PTZ Control. For more information about how to set up the viewing region of the current video stream, please refer to Video settings on page 33.</p>










 <p>ePT Direction</p>	<p>Home: Move the camera to the preset home position.</p> <p>Direction: Control the camera's pan or tilt directions (up/down/left/right).</p>
 <p>Zoom</p>	<p>Zoom in/out to magnify or shrink the digital image.</p> <p> Zoom in: Magnify image</p> <p> Zoom out: Diminish image</p>
 <p>Patrol Auto Pan</p>	<p> Patrol: Patrol executes a pre-defined sequence of pan, tilt, zoom, and focus features Before selecting this, users must define at least two preset points.</p> <p> Auto Pan: Auto Pan automatically scans an area horizontally.</p> <p> Stop: Stop patrol and auto pan</p>
 <p>Go Preset</p>	<p>Select from the preset drop-down list to quickly move the camera to the desired preset position.</p>
 <p>Speed Control</p>	<p>Control Pan/Tilt/Zoom speed</p> <p> Pan Speed Control</p> <p> Tilt Speed Control</p> <p> Zoom Speed Control</p>


*See "Mechanical PTZ" on page 65 for more information about the installation of a PTZ scanner.





 Snapshot	<p>Click this button to capture and save still images. The captured images will be displayed in a pop-up window. Right-click the image and choose Save Picture As to save it in JPEG (*.jpg) or BMP (*.bmp) format.</p>
 Recording	<p>Click this button to record video clips to your computer. When you exit the web browser, video recording stops accordingly.</p>
 Recording Folder	<p>Specify a storage destination for the recorded video files.</p>
 Digital Zoom	<p>Click and uncheck "Disable digital zoom" to enable the zoom operation. The navigation screen indicates the part of the image being magnified. To control the zoom level, drag the slider bar. To move to a different area you want to magnify, drag the navigation screen.</p>
 Full Screen	<p>Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode.</p>
 Zoom ratio	<p>Auto: The video zoom ratio will be changed automatically according to viewing window size. 100%: Keep the video zoom ratio at 100% 50%: Keep the video zoom ratio at 50% 25%: Keep the video zoom ratio at 25%</p>
 Help	<p>Click the Help button to learn the detailed information regarding camera setup and solve any problems you encounter.</p>

Client Setup

Clicking the Client Settings button  will bring you to the following screen which allows you to configure the basic protocol options for your camera.

H.264/MPEG4 Protocol Options

For additional information about streaming options please see page 41.

UDP Unicast: Stream to a single computer.

UDP Multicast: Stream to multiple computers using multicast streaming.

TCP: Provides higher quality video streaming than UDP and provides error correction. However, transmission speed will be reduced.

HTTP: Offers the highest image and video quality. However, packet loss will diminish image quality when bandwidth becomes restricted. If the network is protected by a firewall and it opens only HTTP port (80), HTTP protocol must be selected. In this mode, audio is disabled and only video can be viewed. UDP connections will not be available to remote users if all four ports have not been forwarded (as shown on page 46). Only the HTTP port must be forwarded for remote users to make an HTTP connection (video only).

MP4 Saving Options

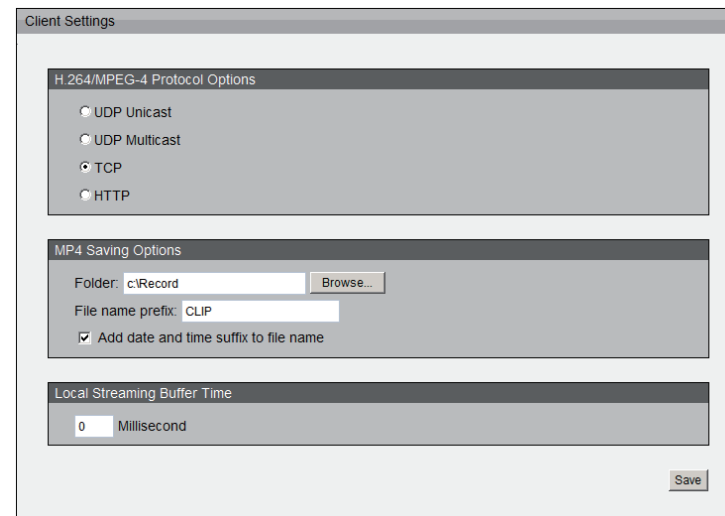
Folder: Select the folder where you would like the MP4 file saved on your desktop computer.

File name prefix: Enter a file name prefix for the MP4 files.

Add date and time suffix to file name: Select this checkbox if you would like the date and time to be added to the end of each filename.

Local Streaming Buffer Time

Enter the buffer time in milliseconds. The buffer will cause a slight delay between live activity and the video of the live stream but may increase the quality of video.



The screenshot shows the 'Client Settings' window with three main sections:

- H.264/MPEG-4 Protocol Options:** A group box containing four radio buttons: 'UDP Unicast', 'UDP Multicast', 'TCP' (which is selected), and 'HTTP'.
- MP4 Saving Options:** A group box containing a 'Folder:' label with a text input field containing 'c:\Record' and a 'Browse...' button, a 'File name prefix:' label with a text input field containing 'CLIP', and a checked checkbox labeled 'Add date and time suffix to file name'.
- Local Streaming Buffer Time:** A group box containing a text input field with the value '0' and the label 'Millisecond'.

A 'Save' button is located at the bottom right of the window.

Setup

The DCS-7110 includes basic and advanced setup screens. Both screens include a tree view with multiple setup options. This manual includes detailed explanations for all advanced setup screens.

Basic Setup

Click the **setup** button to enter the setup screen.



Click on the **basic** button to enter the setup screen.



Please click the [+] next to each folder to view the options.

Basic setup includes the following options:

System Overview

Video

- Video Settings

Network

- IP Settings

Event Management

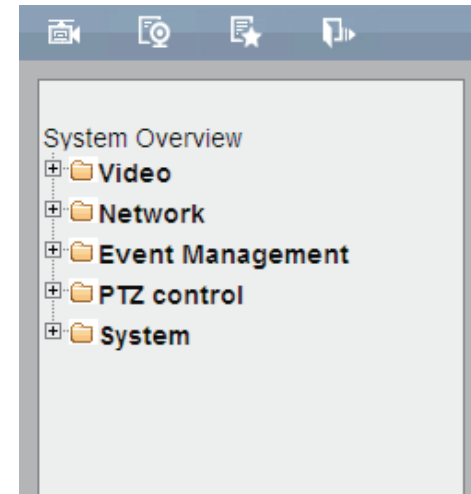
- Motion Detection, Tamper Detection

PTZ Control

- Digital PTZ

System

- User Settings, Device Settings, Time and Date, Maintenance



Advanced Setup

Click the **setup** button to enter the setup screen.



Click on the **advanced** button to enter the setup screen.



Please click the [+] next to each folder to view the options.

Advanced setup includes the following options:

System Overview

Video

- Video Settings, Image Settings, Day and Night Settings

Network

- IP Settings, Port & Access Name Settings, Dynamic DNS, HTTPS, Access List, Advanced Settings

Event Management

- Motion Detection, Tamper Detection, DI and DO, Event Settings

Recording

- Recording Settings

PTZ Control

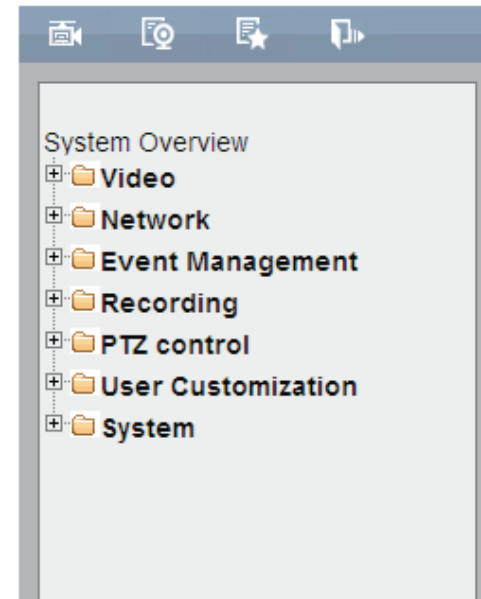
- Digital PTZ, Mechanical PTZ

User Customization

- Live Video Page Config, HTML Code Examples

System

- User Settings, Device Settings, Time and Date, Maintenance, Parameter List, Logs



System Overview

The system overview page contains a summary of the camera's current settings. For more information about adjusting these settings, please consult the subsequent instructions found in this manual.

System Overview

Device Information

IP address	0.0.0.0
Link-local address	169.254.0.99
Current firmware version	v1.00
Current firmware date	1 Nov 2010
MAC address	00:00:83:32:10:15
Connect client	0

Time and Date

Current system time	14 Nov 2010 14:37:45
System up time	0 Days, 0 Hours, 1 Minutes
Time mode	Manually

Service Status

Service	enabled_disabled	Protocol	Server port
HTTP	Enable	TCP	80
Secondary HTTP	Enable	TCP	8080
HTTPS	Disable	TCP	443
FTP	Enable	TCP	21
RTSP	Enable	TCP	554
UPnP presentation	Enable	-	-
UPnP port forwarding	Disable	-	-
802.1x	Disable	-	-
CoS	Disable	-	-
QoS/DSCP	Disable	-	-
SNMP	Disable	-	-
DDNS	Disable	-	-
ACCESS List	Disable	-	-

Stream Status

Stream number	Codec type	Resolution	Max Frame Rate	Bitrate/Quality
Stream 1	H.264	1280x800	30	Good
Stream 2	H.264	640x400	30	2 Mbps
Stream 3	MPEG-4	176x144	5	40 Kbps
Stream 4	H.264	1280x800	30	2 Mbps

Recent Logs

```

Nov 14 14:37:28 [NET]: Secondary DNS =
Nov 14 14:37:28 [SYS]: Recording entry 0 stop
Nov 14 14:37:29 [SYS]: Recording entry 1 stop
Nov 14 14:37:29 [EVENT MGR]: Reload event task config files...
Nov 14 14:37:29 [EVENT MGR]: Task conf file: there is no valid event in recording_task.xml, skip it
Nov 14 14:37:29 [EVENT MGR]: Task conf file: there is no valid event in event_task.xml, skip it
Nov 14 14:37:34 [IR Cut Control]: Day mode
Nov 14 14:37:38 [init]: init: starting pid 862, tty "": /sbin/getty -L ttyS0 115200 vt100
Nov 14 14:37:38 [NIPCA]: Start NipcaFdServer
Nov 14 14:37:45 udhccp: IP 0.0.0.0

```


Video

Video Settings

This page allows you to set up 4 video streams to be displayed on a computer, mobile device, or storage system. Each stream has independent options for proper compression type, frame size, frame rate to optimize the bandwidth utilization and video quality.

Video Options

Viewing Window: The camera supports multiple streams with frame size ranging from 176 x 144 to 1920x1080. Click **Viewing Window** to open the viewing region setting page. On this page, you can set the Region of Interest (ROI) and the Output Frame Size for stream 1~3. Please follow the steps below to set up a stream:

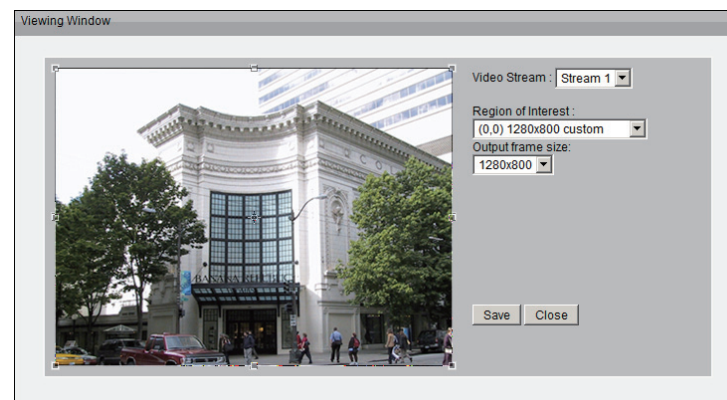
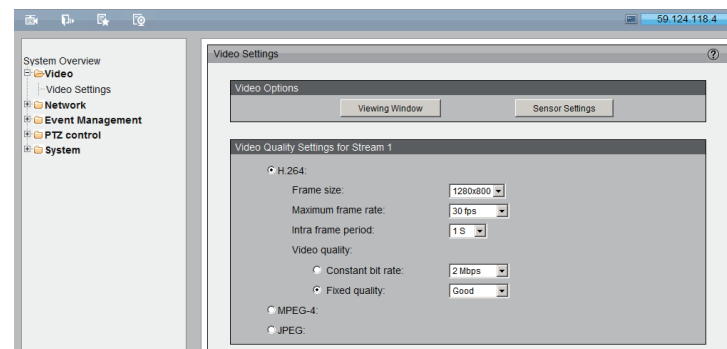
1. Select a stream whose viewing region you would like to set.
2. Select a Region of Interest from the drop-down list, the floating frame will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.
3. Choose a proper Output Frame Size from the drop-down list according to the size of your monitoring device.

Note: All the items in the "Output Frame Size" should not be greater than the "Region of Interest" (current maximum resolution).

The definition of multiple streams:

Stream 1-3: Users can define the "Region of Interest" (viewing region) and the "Output Frame Rate" (size of the live view window).

Stream 4: This is global view stream which captures the full view of the video. Users can also define the "Output Frame Rate" (size of the live view window).



Once finished with the setting in the Viewing Window, click **Save** to enable the settings and click **Close** to exit the window. The selected Output Frame Size will immediately be applied to the Frame size of video stream. You can then go back to the Live Video to test the new settings.

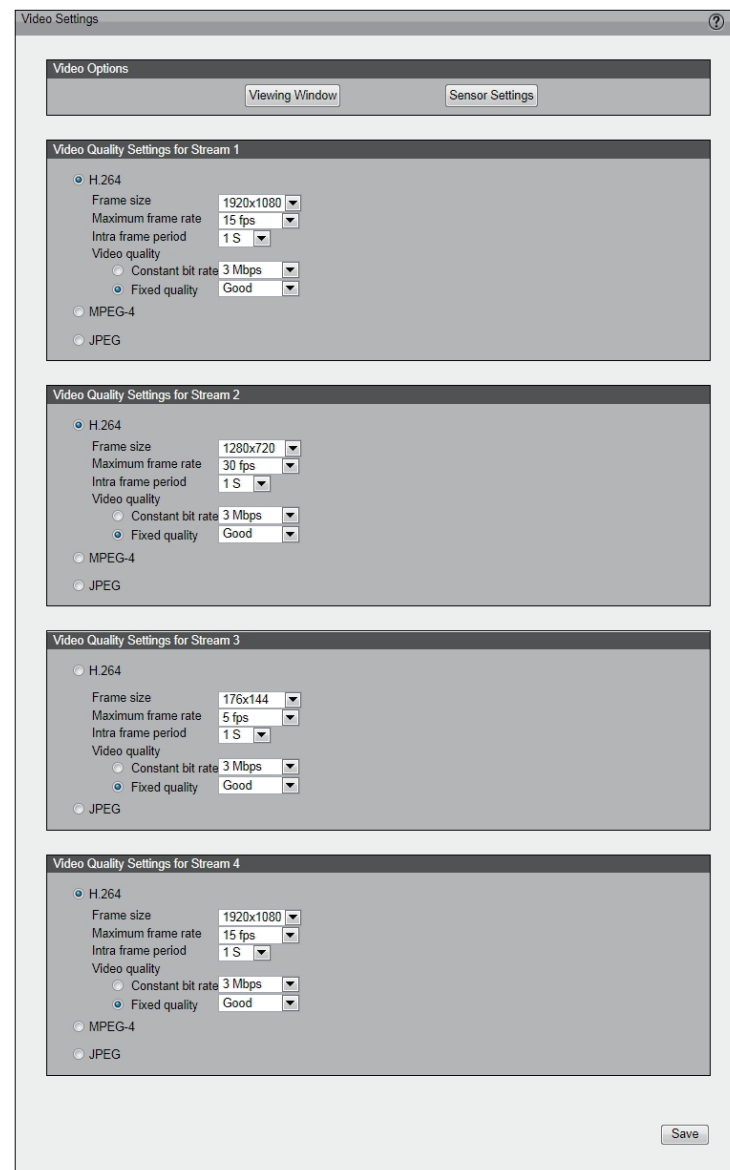
Sensor Setting: Click **Sensor Setting** to open the Sensor Setting page. On this page, you can set the maximum exposure time, exposure level, and AGC (Auto Gain Control) setting. You can configure two sets of sensor setting: one for normal situations, the other for special situations, such as day/night/schedule mode.

Exposure

- **Maximum Exposure Time:** Select a proper maximum exposure time according to the light source of the surroundings. Shorter exposure times result in less light reaching the sensor. The exposure times are selectable for the following durations: 1/30 second, 1/15 second, and 1/5 second.
- **Exposure level:** You can manually set the Exposure level which ranges from 1 to 8 (dark to bright).
- **Max. Gain (Auto Gain Control):** You can manually set the AGC level (2X 4X, or 8X). The higher the value, the brighter the image will be.
- **Enable BLC (Back Light Compensation):** Enable this option when the object is too dark or too bright to recognize. It allows the camera to adjust to the best light conditions in any environment and automatically give the necessary light compensation.

You may click **Preview** to fine-tune the image, or click **Restore** to recall the original setting without incorporating the changes. When completed with the setting on this page, click **Save** to enable the setting and click **Close** to exit the page. If you want to configure another sensor setting for day/night/schedule mode, please click **Profile 2** and follow the steps below to setup:

1. Click Enable this profile.
2. Select the applied mode: Day mode, Night mode, or schedule mode. Please manually enter a range of time if you choose Schedule mode.
3. Configure Exposure setting in the second column.
4. Click **Save** to enable the setting and click **Close** to exit the page.



Video Quality Setting for Stream 1~4

Compression Type: The compression level affects the amount of bandwidth and storage required. Lower compression uses more bandwidth and storage but delivers better image quality. Of the three options, H.264 consumes much less network bandwidth compared to MPEG4 and JPEG.

Frame Size: Select proper frame size for different viewing devices, bigger frame size requires more bandwidth and storage usage. For smaller viewers, such as mobile phones, a smaller frame size and lower frame rate is recommended. There are 5 options you can select: 176x144, 320x240, 640x480, 1280x720 1360x768, 1600x940, 1920x1080, if there is no viewing window applied. (176x144 for mobile phone, 640x480 for VGA display, 1280x720 for HD display).

Frame Rate: This option affects the smoothness of the video. Select higher frame rate for smoother video quality but it requires more storage usage. 10 options for selection: customize, 1, 3, 5, 8, 10, 15, 20, 25, 30 fps (30 fps is recommended real-time video on a computer monitor. 5 fps is ideal for mobile viewers.)

Intra Frame Period: Determines the frequency and I frame is planted. The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds and 4 seconds.

Video Quality: This setting limits the maximum refresh frame rate.

- **Constant bit rate:** To set a fixed bandwidth regardless of the video quality, select Constant bit rate and the desired bandwidth from 20 Kbps to 8 Mbps. You can also select **Customize** and manually enter a value.
- **Fixed quality:** To optimize the bandwidth utilization and video quality. The video quality can be adjusted to the following setting: Medium, Standard, Good, Detailed and Excellent. You can also select **Customize** and manually enter a value.

The screenshot displays the 'Video Settings' window with four sections for Stream 1, Stream 2, Stream 3, and Stream 4. Each section is identical in layout, featuring a 'Video Options' header with 'Viewing Window' and 'Sensor Settings' buttons. Below this, the 'Video Quality Settings for Stream X' section is shown. Each stream is configured with H.264 as the compression type. Stream 1 and 2 have a frame size of 1280x800, a maximum frame rate of 30 fps, an intra frame period of 1 S, and a video quality of 'Good'. Stream 3 has a frame size of 1280x800, a maximum frame rate of 30 fps, an intra frame period of 1 S, and a video quality of 'Detailed'. Stream 4 has a frame size of 1280x800, a maximum frame rate of 30 fps, an intra frame period of 1 S, and a video quality of 'Detailed'. All streams have 'Constant bit rate' selected with a value of 2 Mbps, except for Stream 3 which is set to 40 Kbps. The 'MPEG-4' and 'JPEG' options are unselected for all streams.

Save

Image Settings

This page allows you to tune the white balance, brightness, saturation, contrast, and sharpness settings for the video.

Color: Select either a Color or B/W (black and white, monochrome) video display.

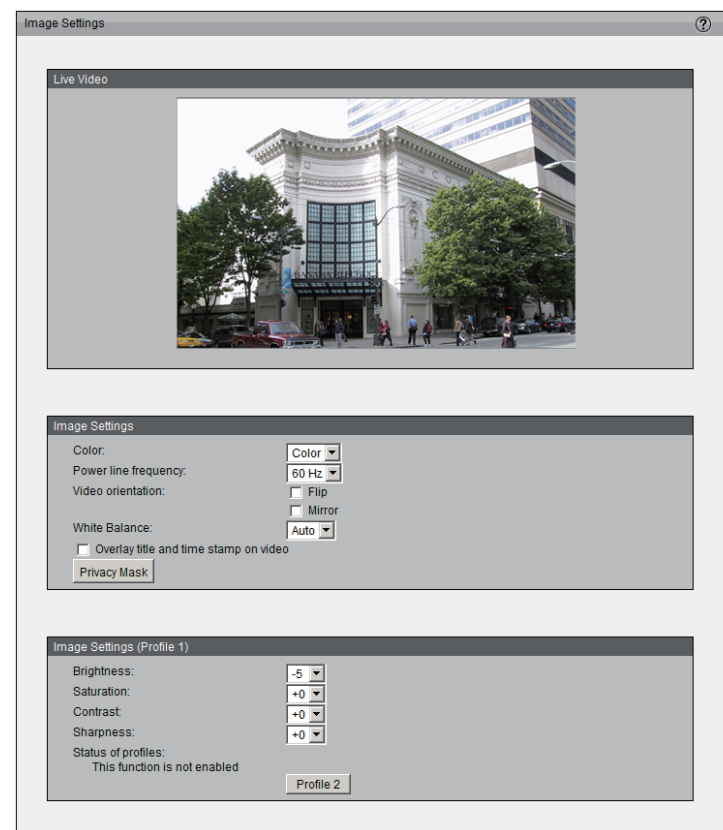
Power Line Frequency: Select either 50 or 60 Hz depending on your region.

Video Orientation: Flip will vertically rotate the video. Mirror will horizontally rotate the video. You may select both options if camera is being installed upside down.

White Balance: This adjusts the relative amount of red, green and blue primary colors in the image so that the neutral colors are reproduced correctly.

- **Auto:** The camera automatically adjusts the color temperature of the light in response to different light sources. The white balance setting defaults to Auto and works well in most situations.
- **Fixed:** Follow the steps below to manually set the white balance to compensate for the ambient lighting conditions

1. Set the White balance to Auto and click **Save**.
2. Place a sheet of white paper in front of the lens, then allow the camera to adjust the color temperature automatically.
3. Select Fixed to confirm the setting while the white balance is being measured.
4. Click **Save** to enable the new setting.



Brightness: Adjust the image brightness level, which ranges from -5 to +5

Saturation: Adjust the image saturation level, which ranges from -5 to +5

Contrast: Adjust the image contrast level, which ranges from -5 to +5

Sharpness: Adjust the image sharpness level, which ranges from -3 to +3

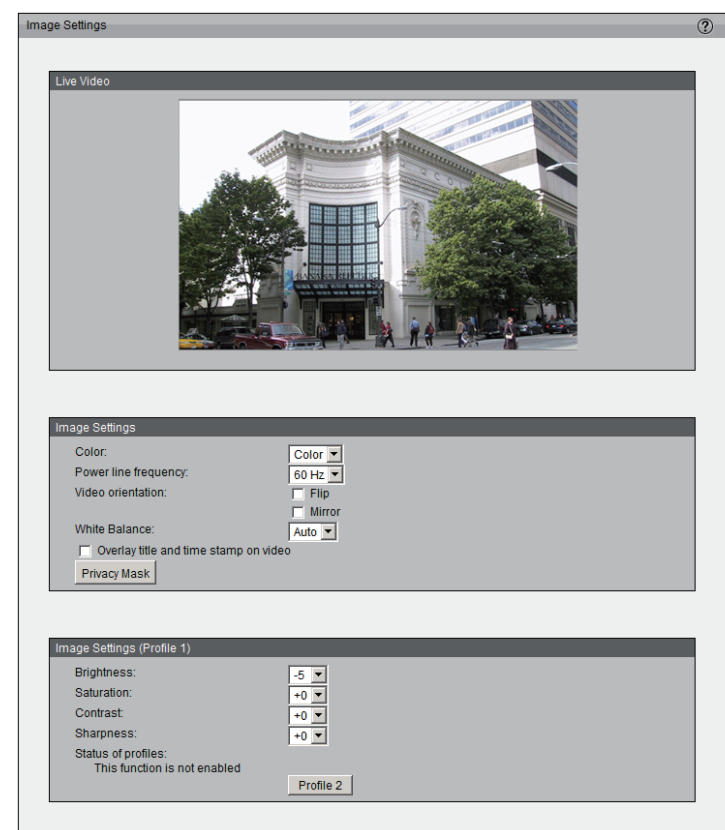
Overlay Title and Time Stamp on Video: Select this option to place the video title and time on the video streams. (When the frame size is set to 176 x 144 only the time will be stamped on the video streams.)

Privacy Mask: In this page, you can block out certain sensitive zones for privacy concerns. To set up a Privacy Mask Window, follow the steps given below:

1. Click **New** to add a window.
2. The height and width of the window can be resized and drag-dropped the window.
3. Enter a descriptive Window Name and click **Save** to apply changes.
4. Select Enable privacy mask to facilitate this function.

None:

- Up to 5 privacy mask windows can be set up on the same screen.
- If you want to delete the privacy mask window, please click the 'x' at the upper right-hand corner of the window.



Day and Night Settings

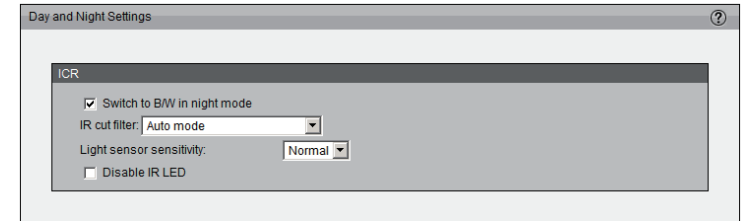
Switch to B/W in Night Mode: Select to automatically enable the camera to switch to B/W night mode.

IR Cut Filter: The IR-Cut Removable (ICR) filter mechanically switches between two different sensor filters. It provides the best light conditions both during the day and night. The following options are:

- **Auto Mode:** The camera automatically switches between day and night mode by judging the level of ambient light. This mode is accessible only when the exposure mode is set to Auto.
- **Day Mode:** In this mode the camera switches on the IR cut filter at all times, which will block the infrared light from reaching the sensor so that the colors are not distorted.
- **Night Mode:** The camera switches off the IR cut filter to allow the infrared light to pass through. This helps the camera to see more clearly in low light conditions.
- **Synchronize with Digital Input:** The camera automatically removes the IR cut filter when DI triggers.
- **Schedule Mode:** The camera switches between day and night mode based on a specific schedule. Ensure to enter the starting and ending time for the day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the starting time and ending time of day mode are set to 07:00 and 18:00.

Light Sensor Sensitivity: Select Low, Normal, or High sensitivity for the light sensor.

Disable IR LED: Select this box to disable the IR LED. The IR LED automatically switches on at night. By default the LED automatically switches on at night.



Save

Network

IP Settings

IPv4

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

- **Get IP address automatically (DHCP):** Select this connection if you have a DHCP server running on your network and would like a dynamic IP address to be assigned to the camera automatically.
- **Use fixed IP address:** You may enter a static or fixed IP address for your camera.

IP Address: Enter an IP address.

Subnet Mask: The default value is "255.255.255.0." This helps to determine if the designated IP address is on the same subnet.

Default Router: This is the gateway used to forward frames to destinations in a different subnet. (Invalid router setting will cause the transmission to fail if its destination is in a different subnet).

Primary DNS: The Primary Domain Name Server (DNS) that translates hostname into IP address.

Secondary DNS: Secondary Domain Name Server (DNS) that backups the Primary DNS.

Primary WINS Server: The primary WINS server that maintains the database of computer name and IP address.

Secondary WINS Server: The secondary WINS server that maintains the database of

IP Settings

IPv4

LAN:

- Get IP address automatically
- Use fixed IP address:
 - Enable UPnP presentation
 - Enable UPnP port forwarding
- PPPoE:

IPv6

Enable IPv6

Save

IP Settings

IPv4

LAN:

- Get IP address automatically
- Use fixed IP address:

IP address:	59.124.118.4
Subnet mask:	255.255.255.248
Default router:	59.124.118.1
Primary DNS:	168.95.1.1
Secondary DNS:	139.175.55.244
Primary WINS server:	
Secondary WINS server:	
- PPPoE:

Enable UPnP presentation

Enable UPnP port forwarding

IPv6

Enable IPv6

Save

computer name and IP address.

- **Enable UPnP Presentation:** Select this option to enable UPnP presentation for the camera so that whenever a camera is presented to the LAN, shortcuts of connected cameras will be listed in My Network Places. You can click the shortcut to link to the web browser. Currently, UPnP is supported by Windows XP or later. Note that to utilize this feature, please make sure the UPnP component is installed on your computer.
- **Enable UPnP Port Forwarding:** To access the camera from the Internet, select this option to allow the camera to open ports on the router automatically so that video streams can be sent out from a LAN. To utilize this feature, make sure that your router supports UPnP and it is activated.

How does UPnP work?

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

PPPoE: Select this option to configure the camera to make it accessible from anywhere with an Internet connection. Note that to utilize this feature, it requires an account provided by your ISP.

Follow the steps below to acquire the camera's public IP address.

1. Set up the camera on the LAN
2. Go to **Live View > Setup > Event management > Event settings > Server Settings** (please refer to Server Settings to add a new e-mail or FTP server)
3. Go to **Setup > Event management > Event settings > Media Settings** (please refer to Media Settings). Select System log so that you will receive the system log in TXT file format which contains the camera's public IP address in your e-mail or on the FTP server.
4. Go to **Setup > Network > IP settings**. Select PPPoE and enter the user name and password provided by your ISP. Click **Save** to enable the setting.

The screenshot shows the 'IP Settings' window with the 'IPv4' section selected. Under 'LAN', the 'Use fixed IP address' option is chosen. The fields are filled with: IP address: 59.124.118.4, Subnet mask: 255.255.255.248, Default router: 59.124.118.1, Primary DNS: 168.95.1.1, and Secondary DNS: 139.175.55.244. The 'Enable UPnP presentation' and 'Enable UPnP port forwarding' checkboxes are unchecked. The 'PPPoE' option is not selected. A 'Save' button is visible at the bottom right.

The screenshot shows the 'IP Settings' window with the 'PPPoE' option selected. The 'User name' field contains '123456@hinet.net'. The 'Password' and 'Confirm password' fields are masked with dots.

5. The camera will reboot.
6. Disconnect the power to the camera. Remove it from the LAN environment.

IPv6

Enable IPv6: Select this option and click **Save** to enable IPv6 setting. Please note that this only works if your network environment and hardware equipment support IPv6. The browser should be Microsoft® Internet Explorer 6.5, Mozilla Firefox 3.0 or above.

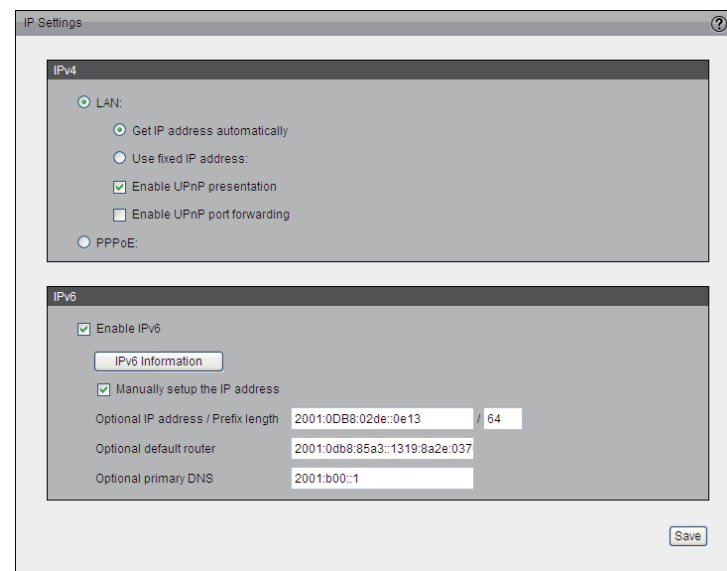
When IPv6 is enabled, by default, the camera will listen to router advertisements and be assigned a link-local IPv6 address accordingly.

IPv6 Information: Click this button to obtain the IPv6 information. If your IPv6 setting are successful, the IPv6 address list will be listed in the pop-up window.

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

1. Open your web browser.
2. Enter the link-global or link-local IPv6 address in the address bar of your web browser.
3. Press **Enter** on the keyboard or click **Refresh** button to refresh the webpage.

Manually Setup the IP Address: Select this option to manually configure IPv6 setting if your network environment does not have DHCPv6 server and advertisements-enabled routers.



The screenshot displays the 'IP Settings' window, which is divided into two main sections: IPv4 and IPv6. The IPv4 section is currently selected and shows the following options: 'LAN' (selected), 'Get IP address automatically' (selected), 'Use fixed IP address:' (unselected), 'Enable UPnP presentation' (checked), 'Enable UPnP port forwarding' (unchecked), and 'PPPoE:' (unselected). The IPv6 section shows 'Enable IPv6' (checked), an 'IPv6 Information' button, 'Manually setup the IP address' (checked), and three input fields: 'Optional IP address / Prefix length' with the value '2001:0DB8:02de::0e13 / 64', 'Optional default router' with the value '2001:0db8:85a3::1319:8a2e:037', and 'Optional primary DNS' with the value '2001:b00::1'. A 'Save' button is located at the bottom right of the IPv6 section.

Port and Access Name Settings

HTTPS

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

FTP

The FTP server allows the user to save recorded video clips. You can utilize D-Link's IP Cam Wizard to upgrade the firmware via FTP server. By default, the FTP port is set to 21. It also can be assigned to another port number between 1025 and 65535.

HTTP

By default, the HTTP port is set to 80 and the secondary HTTP port is set to 8080. They can also be assigned to another port number between 1025 and 65535.

Authentication: Depending on your network security requirements, the camera provides two types of security setting for an HTTP transaction: basic and digest. If basic authentication is selected, the password is sent in plain text format and there can be potential risks of being intercepted. If digest authentication is selected, user credentials are encrypted using MD5 algorithm and thus provide better protection against unauthorized accesses.

Access name for stream 1 ~ 5: The Network camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. Users can click **Setup > Video > Video Settings** to set up the video quality of linked streams.

RTSP

To utilize RTSP streaming authentication, make sure that you have set a password for the camera first. Please refer to User Settings for details.

Authentication: Depending on your network security requirements, the camera provides three types of security setting for streaming via RTSP Protocol: disable,

The screenshot shows the 'Port & Access Name Settings' window with the following configurations:

- HTTPS:** HTTPS port: 443
- FTP:** FTP port: 21
- HTTP:**
 - Authentication: basic
 - HTTP port: 80
 - Secondary HTTP port: 9000
 - Access name for stream 1: video.mjpg
 - Access name for stream 2: video2.mjpg
 - Access name for stream 3: video3.mjpg
 - Access name for stream 4: video4.mjpg
 - Access name for stream 5: videoany.mjpg
- RTSP Streaming:**
 - Authentication: disable
 - Access name for stream 1: live.sdp
 - Access name for stream 2: live2.sdp
 - Access name for stream 3: live3.sdp
 - Access name for stream 4: live4.sdp
 - Access name for stream 5: liveany.sdp
 - RTSP port: 554
 - RTP port for video: 5556
 - RTCP port for video: 5557
- Multicast:**
 - Enable multicast for stream 1
 - Multicast group address: 239.128.1.99
 - Multicast video port: 5560
 - Multicast RTCP video port: 5561
 - Multicast TTL [1~255]: 15
 - Enable multicast for stream 2
 - Enable multicast for stream 3
 - Enable multicast for stream 4

A 'Save' button is located at the bottom right of the window.

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

Access Name for Stream 1 ~ 5: This camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. If you want to use an RTSP player to access the camera, you have to set the video mode to H.264 / MPEG-4 and use the following RTSP URL command to request transmission of the streaming data.

Multicast and Unicast Streaming Protocols

You may choose to enable multicast or unicast for your camera audio and video streaming so that your cameras (sources) and the receivers (clients) can establish the connection to send and receive contents.

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

An IP Multicast group address is used to send and receive content. Sources use this group address as the destination address while sending their data packets. Receivers use this group address to inform the network that they are interested in receiving packets sent to that group.

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

Port & Access Name Settings

HTTPS
HTTPS port: 443

FTP
FTP port: 21

HTTP
Authentication: basic
HTTP port: 80
Secondary HTTP port: 9000
Access name for stream 1: video.mjpg
Access name for stream 2: video2.mjpg
Access name for stream 3: video3.mjpg
Access name for stream 4: video4.mjpg
Access name for stream 5: videoany.mjpg

RTSP Streaming
Authentication: disable
Access name for stream 1: live.sdp
Access name for stream 2: live2.sdp
Access name for stream 3: live3.sdp
Access name for stream 4: live4.sdp
Access name for stream 5: liveany.sdp
RTSP port: 554
RTP port for video: 5556
RTCP port for video: 5557

Multicast
 Enable multicast for stream 1
Multicast group address: 239.128.1.99
Multicast video port: 5560
Multicast RTCP video port: 5561
Multicast TTL [1~255]: 15
 Enable multicast for stream 2
 Enable multicast for stream 3
 Enable multicast for stream 4

Save

changes, the multicast RTCP port will change accordingly.

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

Click the items to display the detailed configuration information. Select the **Always multicast** option to enable multicast for stream 1 ~ 4.

Dynamic DNS

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

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

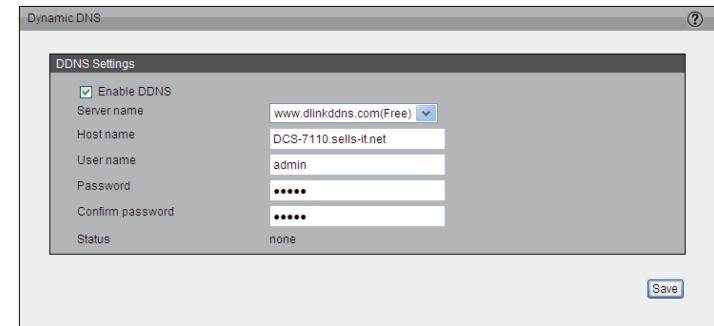
Server Name: Select a DDNS server name from the provider drop-down list. With a Dynamic DNS account, the camera automatically updates your IP address. To enable DDNS, enter your host information. Click **Next** to continue.

Host Name: Enter the host name of the DDNS server.

Username: Enter your username or e-mail used to connect to the DDNS

Password: Enter your password used to connect to the DDNS server.

Status: Indicate the connection status, automatically determined by the system.



The screenshot shows a web-based configuration window titled "Dynamic DNS". Inside the window, there is a section titled "DDNS Settings". The settings are as follows:

Field	Value
Enable DDNS	<input checked="" type="checkbox"/>
Server name	www.dlinkddns.com(Free)
Host name	DCS-7110.sells-it.net
User name	admin
Password	•••••
Confirm password	•••••
Status	none

A "Save" button is located at the bottom right of the configuration area.

HTTPS

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

Enable HTTPS

Select this item to enable HTTPS communication, then select a connection option: "HTTP & HTTPS" or "HTTPS only". Note that you have to create and install a certificate first in the second column before clicking the **Save** button.

Create and Install Certificate Method

Before using HTTPS for communication with the camera, a certificate must be created first.

There are three ways to create and install a certificate:

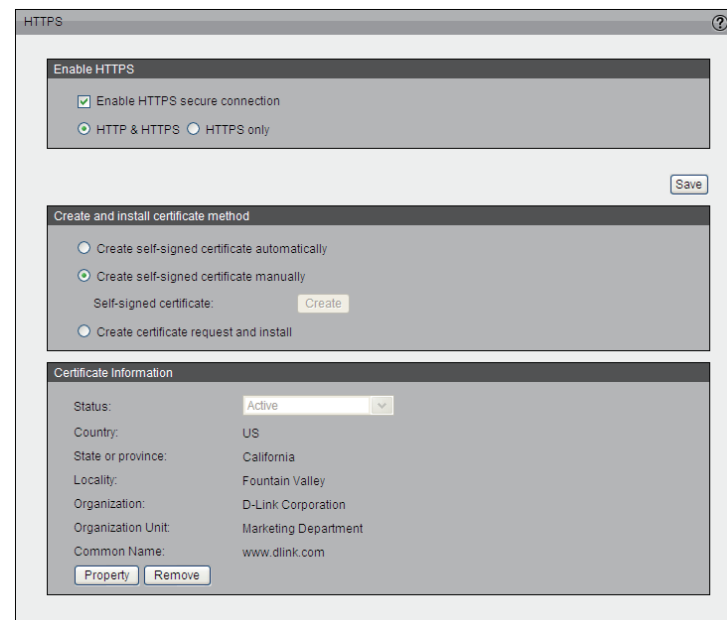
Create Self-signed Certificate Automatically

1. Select this option.
2. In the first column, select **Enable HTTPS secure connection**, then select a connection option: "HTTP & HTTPS" or "HTTPS only".
3. Click **Save** to generate a certificate.
4. The **Certificate Information** will automatically be displayed in the third column. You can click **Property** to view detailed information about the certificate.
5. Click **Live Video** to return to the main page. Change the address from "http://" to "https://" in the address bar and press Enter. Some Security Alert dialogs will pop up. Click **OK** or **Yes** to enable HTTPS.

Create Self-signed Certificate Manually

1. Click **Create** to open the Create Certificate page, then click **Save** to generate the certificate.
2. The Certificate Information will automatically be displayed in the third column as shown below. You can click **Property** to see detailed information about the certificate.

Create Certificate Request and Install



The screenshot shows the HTTPS configuration page with three main sections:

- Enable HTTPS:** A checkbox for "Enable HTTPS secure connection" is checked. Below it are two radio buttons: "HTTP & HTTPS" (selected) and "HTTPS only". A "Save" button is located to the right.
- Create and install certificate method:** Three radio buttons are present: "Create self-signed certificate automatically", "Create self-signed certificate manually" (selected), and "Create certificate request and install". A "Create" button is next to the "Self-signed certificate:" label.
- Certificate Information:** A table-like view showing certificate details:

Status:	Active
Country:	US
State or province:	California
Locality:	Fountain Valley
Organization:	D-Link Corporation
Organization Unit:	Marketing Department
Common Name:	www.dlink.com

Buttons for "Property" and "Remove" are at the bottom.

Select this option to create a certificate from a certificate authority.

1. Click **Create** to open the **Create Certificate** page, then click **Save** to generate the certificate.
2. If you see the information bar, click **OK** and click on the Information bar at the top of the page to allow pop-up.
3. The pop-up window shows an example of a certificate request.
4. Look for a trusted certificate authority that issues digital certificates. Enroll the camera.

Wait for the certificate authority to issue a SSL certificate. Click **Browse...** to search for the issued certificate, then click **Upload** in the second column.

How do I cancel the HTTPS setting?

1. Deselect **Enable HTTPS secure connection** in the first column and click **Save**. A warning dialog will pop up.
2. Click **OK** to disable HTTPS.
3. The webpage will redirect to a non-HTTPS page automatically.

If you want to create and install other certificates, please remove the existing one. To remove the signed certificate, deselect **Enable HTTPS secure connection** in the first column and click **Save**. Then click **Remove** to erase the certificate.

The screenshot shows the HTTPS configuration interface. It includes the following elements:

- Enable HTTPS:** A checked checkbox for "Enable HTTPS secure connection". Radio buttons for "HTTP & HTTPS" (selected) and "HTTPS only". A "Save" button.
- Create and install certificate method:** Radio buttons for "Create self-signed certificate automatically", "Create self-signed certificate manually" (selected), and "Create certificate request and install". A "Create" button is next to the "Create self-signed certificate manually" option.
- Certificate Information:** A table with the following fields:

Status:	Active
Country:	US
State or province:	California
Locality:	Fountain Valley
Organization:	D-Link Corporation
Organization Unit:	Marketing Department
Common Name:	www.dlink.com

Buttons for "Property" and "Remove" are located below the table.

Access List

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

General Settings

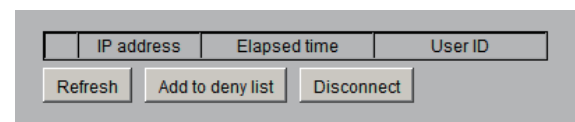
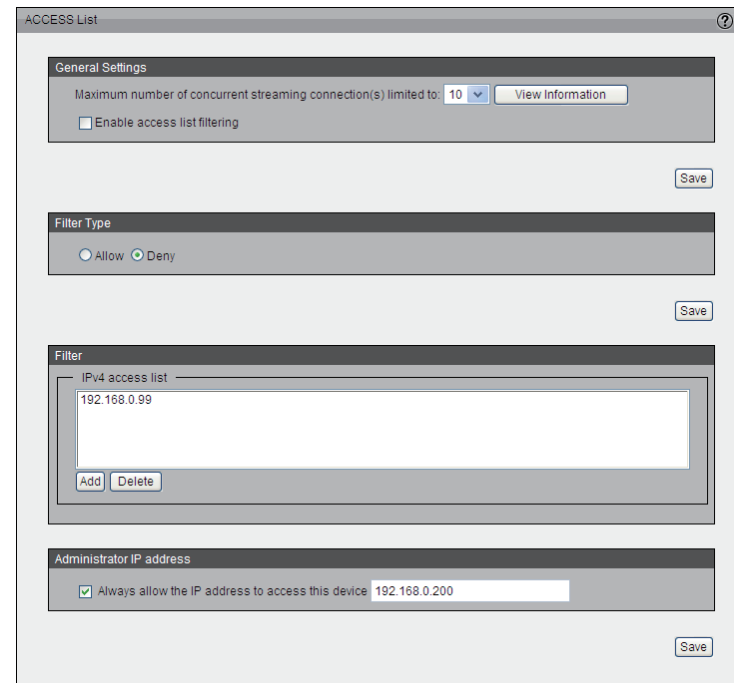
Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 ~ stream 5). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (I.E. Explorer or Quick Time Player).

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

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

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

1. The administrator did not set up a user password. For more information about how to set up a user password and manage user accounts, please refer to User settings.
 2. The administrator has set up a user password, but set RTSP Authentication to "disable". For more information about RTSP Authentication, please refer to RTSP Streaming.
- **Refresh:** Click this button to refresh all current connections.



- **Add to deny list:** You can select entries from the Connection Status list and add them to the Deny List to deny access. Please note that the selected connections will only be disconnected temporarily and will automatically try to re-link again (IE Explore or Quick Time Player). If you want to enable the denied list, please select **Enable access list filtering** and click **Save** in the first column.

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

Enable Access List Filtering: Select this item and click **Save** if you want to enable the access list filtering function.

Filter Type

Select Allow or Deny as the filter type. If you choose Allow Type, only those clients whose IP addresses are on the Access List below can access the camera, and the others cannot access. On the contrary, if you choose Deny Type, those clients whose IP addresses are on the Access List below will not be allowed to access the camera, and the others can access.

Filter

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

There are three types of rules:

Single: This rule allows the user to add an IP address to the Allowed/Denied list.

Network: This rule allows the user to assign a network address and corresponding subnet mask to the Allow/Deny List.

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

Administrator IP address

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

Advanced Settings

SNMP configuration

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

The SNMP consists of the following three key components:

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

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

Enable SNMPv1, SNMPv2c: Select this option and enter the names of Read/Write community and Read Only community according to your NMS setting.

Enable SNMPv3: This option contains cryptographic security, a higher security level which allows you to set the Authentication password and the Encryption password.

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

IEEE 802.1x

Enable this function if your network environment uses IEEE 802.1x which is a port-

The screenshot displays the 'Advanced Settings' web interface with the following sections:

- SNMP Configuration:**
 - Enable SNMPv1, SNMPv2c
 - Read/Write community: Private
 - Read only community: Public
 - Enable SNMPv3
 - Read/Write Security name: Private
 - Authentication Type: MD5
 - Authentication Password: [text input]
 - Encryption Password: [text input]
 - Read only Security name: Public
 - Authentication Type: MD5
 - Authentication Password: [text input]
 - Encryption Password: [text input]
- IEEE 802.1x:**
 - Enable IEEE 802.1x
 - EAP method: EAP-PEAP
 - Identity: [text input]
 - Password: [text input]
 - CA certificate: [text input] [Browse...] [Upload]
 - Status: no file [Remove]
- CoS:**
 - Enable CoS
 - VLAN ID: 1
 - Live Video: 0
 - Event/Alarm: 0
 - Management: 0
- QoS/DSCP:**
 - Enable QoS/DSCP
 - Live Video: 0
 - Event/Alarm: 0
 - Management: 0

Each section has a 'Save' button at the bottom right.

based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x setting.

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

Please follow the steps below to enable 802.1x setting:

1. Before connecting the camera to the protected network with 802.1x, please apply a digital certificate from a Certificate Authority (ie. MIS of your company) which can be validated by a RADIUS server.
2. Connect the camera to a PC or notebook outside of the protected LAN. Open the configuration page of the camera as shown below. Select EAP-PEAP or EAP-TLS as the EAP method. In the following blanks, enter your ID and password issued by the CA, then upload related certificate(s).
3. When all setting are complete, move the camera to the protected LAN by connecting it to an 802.1x enabled switch. The devices will then start the authentication automatically.

QoS (Quality of Service)

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

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

The ability to prioritize traffic and guarantee a certain level of performance to the data flow.

The ability to control the amount of bandwidth each application may use, and thus

The screenshot displays the 'Advanced Settings' window of a camera's configuration interface. It is divided into four main sections:

- SNMP Configuration:** Contains two sub-sections. The first, 'Enable SNMPv1, SNMPv2c', has 'Read/Write community' set to 'Private' and 'Read only community' set to 'Public'. The second, 'Enable SNMPv3', has 'Read/Write Security name' set to 'Private', 'Authentication Type' set to 'MD5', and 'Read only Security name' set to 'Public'. Both sections have fields for 'Authentication Password' and 'Encryption Password'.
- IEEE 802.1x:** Features a checked 'Enable IEEE 802.1x' option. The 'EAP method' is set to 'EAP-PEAP'. There are fields for 'Identity' and 'Password'. A 'CA certificate' field includes 'Browse...' and 'Upload' buttons. The status is 'no file' with a 'Remove' button.
- CoS:** Has a checked 'Enable CoS' option. The 'VLAN ID' is set to '1'. 'Live Video', 'Event/Alarm', and 'Management' are each set to '0' via dropdown menus.
- QoS/DSCP:** Has a checked 'Enable QoS/DSCP' option. 'Live Video', 'Event/Alarm', and 'Management' are each set to '0' via input fields.

'Save' buttons are located at the bottom right of the 'SNMP Configuration' and 'QoS/DSCP' sections.

provide higher reliability and stability on the network.

Requirements for QoS:

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

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

CoS

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

Please follow the steps below to enable CoS settings:

1. Click Enable CoS
2. Enter the VLAN ID of your switch (0~4095)
3. Choose the priority for each application (0~7).

Note:

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

QoS/DSCP

DSCP-ECN defines QoS at Layer 3 (Network Layer). The Differentiated Services (DiffServ) model is based on packet marking and router queuing disciplines. The marking is done by adding a field to the IP header, called the DSCP (Differentiated Services Code Point). This is a 6-bit field that provides 64 different class IDs. It gives an indication of how a given packet is to be forwarded, known as the Per Hop Behavior (PHB). The PHB describes a particular service level in terms of bandwidth,

The screenshot displays the 'Advanced Settings' configuration page, which is divided into several sections:

- SNMP Configuration:** This section contains two sub-sections. The first is for SNMPv1 and SNMPv2c, with 'Enable SNMPv1, SNMPv2c' checked. It includes fields for 'Read/Write community' (set to 'Private') and 'Read only community' (set to 'Public'). The second sub-section is for SNMPv3, with 'Enable SNMPv3' checked. It includes fields for 'Read/Write Security name' (set to 'Private'), 'Authentication Type' (set to 'MD5'), 'Authentication Password', 'Encryption Password', 'Read only Security name' (set to 'Public'), and another 'Authentication Type' (set to 'MD5').
- IEEE 802.1x:** This section has 'Enable IEEE 802.1x' checked. It includes a dropdown for 'EAP method' (set to 'EAP-PEAP'), 'Identity' and 'Password' text boxes, a 'CA certificate' field with 'Browse...' and 'Upload' buttons, and a 'Status' field showing 'no file' with a 'Remove' button.
- CoS:** This section has 'Enable CoS' checked. It includes a 'VLAN ID' text box (set to '1') and three dropdown menus for 'Live Video', 'Event/Alarm', and 'Management', all set to '0'.
- QoS/DSCP:** This section has 'Enable QoS/DSCP' checked. It includes three text boxes for 'Live Video', 'Event/Alarm', and 'Management', all set to '0'.

Each section has a 'Save' button located at the bottom right of the page.

queuing theory, and dropping (discarding the packet) decisions. Routers at each network node classify packets according to their DSCP value and give them a particular forwarding treatment. For example, how much bandwidth should be reserved.

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

Event Management

Motion Detection

Motion can be detected by measuring change in speed or vector of an object or objects in the field of view.

Enable Motion Detection: Select this option to turn on the motion detection feature.

Window Name: Create your own name for the monitored area/ window. It will show at the top of the motion window.

Sensitivity: Set the measurable difference between two sequential images that would indicate motion.

Percentage: Set the amount of motion in the window being monitored that is required to trigger a motion detected alert. If this is set to 100%, this means that motion must be detected within the whole window to trigger a snapshot.

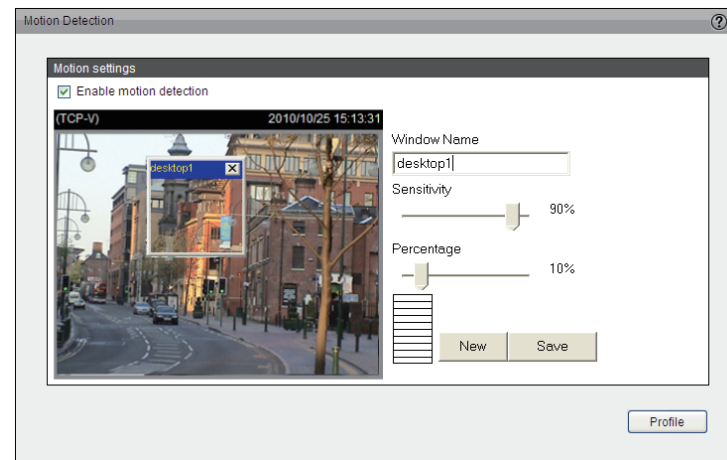
Note: Setting a higher sensitivity and a lower percentage will make motion easier to be detected.

New: Click to add a new window. A maximum of three motion windows can be opened simultaneously. Use your mouse to drag the window frame to resize or the title bar to move. Clicking on the 'x' at the upper right corner of the window will close the window.

Save: Save the configured settings.

To enable motion detection, follow the steps below:

1. Click **New** to add a new motion detection window.
2. Enter a name in the Window Name field.
3. Define the sensitivity to moving objects and the space ratio of all alerted pixels by moving the Sensitivity and Percentage slide bar.
4. Click **Save** to apply the changes.
5. Select Enable motion detection to activate motion detection.



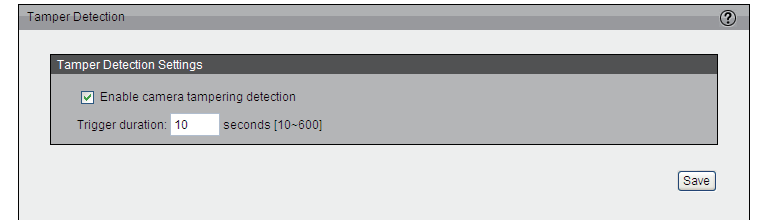
Tamper Detection

With tamper detection, the camera is capable of detecting incidents such as redirection, blocking or de-focusing, or even spray paint.

To enable tamper detection, follow the steps given below:

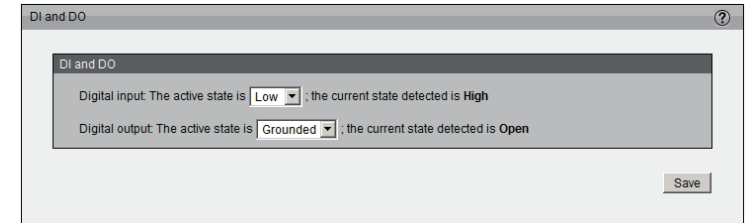
1. Select **Enable camera tampering detection**.
2. Enter the tamper trigger duration (10 sec. ~ 10 min.). The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.

Set up the event source as Camera Tampering Detection on Event Settings > Server Settings (how to send alarm message)/ Media Settings (send what type of alarm message)/Event Settings/. Please refer to Event settings for detailed information.

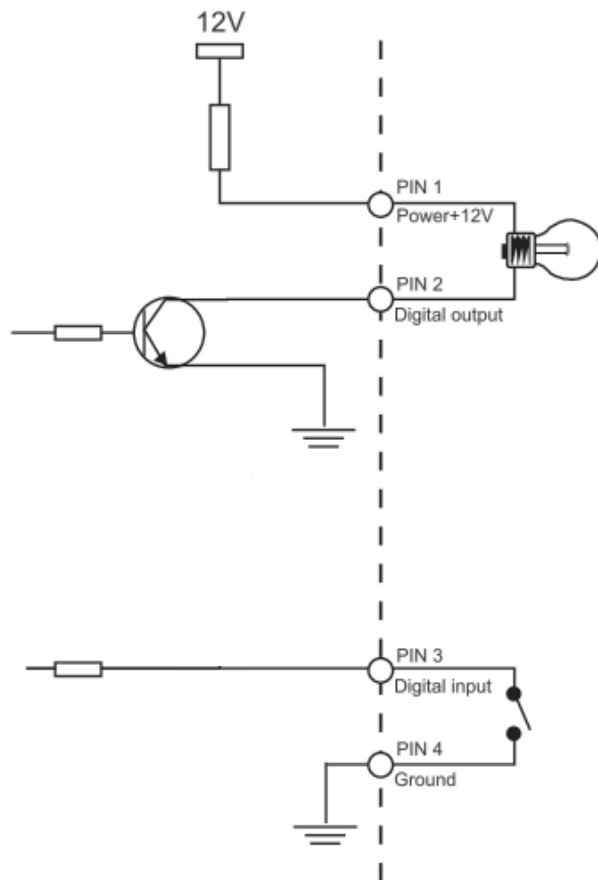


DI and DO

Network camera provides a general I/O terminal block with one digital input and digital output for device control. The I/O connector provides the physical interface for digital input (DI+, GND) and digital output (DO-, +12V) that is used for connecting a diversity of external alarm devices to the camera such as IR-Sensors and alarm relays. Once triggered images will be taken and e-mailed.



DI/DO Schematics



Event Settings

This section explains how to configure the camera to respond to particular situations (event). A typical application is that when a motion is detected, the camera sends buffered images to an FTP server or e-mail address as notifications.

Server Settings

Click **Add Server** on Event Settings page to open the Server Setting page. On this page, you can specify where the notification messages are sent when a trigger is activated. A total of 5 server settings can be configured.

Server name: Enter a name for the server setting.

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

E-mail: Select to send the media files via e-mail when a trigger is activated.

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

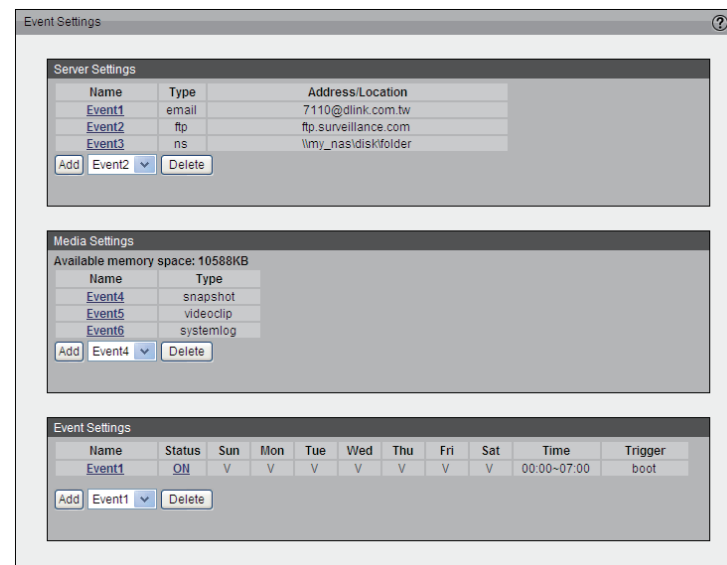
If your SMTP server requires a secure connection (SSL), select **This server requires a secure connection (SSL)**.

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

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

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

- **Server address:** Enter the domain name or IP address of the FTP server.



- **Server port:** By default, the FTP server port is set to 21. It can also be assigned to another port number between 1025 and 65535.
- **User name:** Enter the login name of the FTP account.
- **Password:** Enter the password of the FTP account.
- **FTP folder name:** Enter the folder where the media file will be placed. If the folder name does not exist, the camera will create one on the FTP server.
- **Passive mode:** Most firewalls do not accept new connections initiated from external requests. If the FTP server supports passive mode, select this option to enable passive mode FTP and allow data transmission to pass through the firewall.

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

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

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

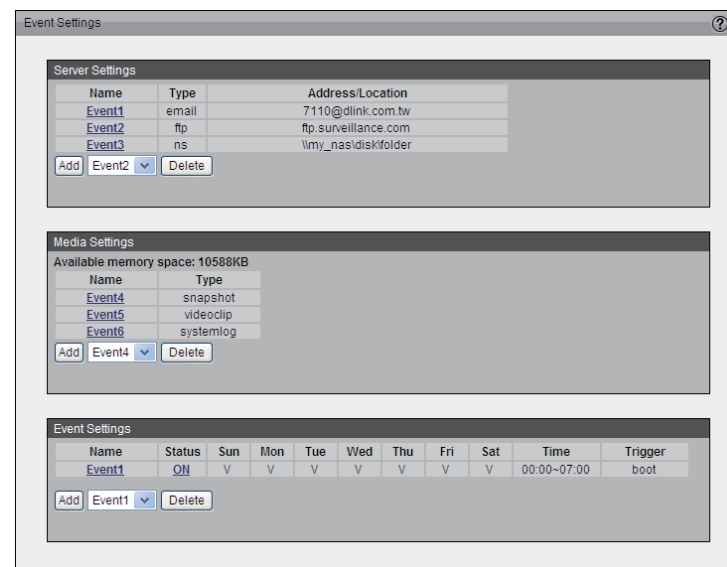
- **URL:** Enter the URL of the HTTP server.
- **User name:** Enter the user name if necessary.
- **Password:** Enter the password if necessary.

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

Network storage: Select to send the media files to a network storage location when a trigger is activated. Click **Save** to enable the setting, then click **Close** to exit the page. When completed, the new server settings will automatically be displayed on the Event Settings page.

Media Settings

Click **Add Media** to open the Media Settings page. On this page, you can specify the type of media that will be sent when a trigger is activated. A total of 5 media settings can be configured.



Configuration

Media name: Enter a name for the media setting.

Media Type: There are three choices of media types available: Snapshot, Video Clip, and System log. Select the item to display the detailed configuration options. You can configure either one or all of them.

Snapshot: Select to send snapshots when a trigger is activated.

Source: Select to take snapshots from stream 1 ~ 4.

Send pre-event images: The camera has a buffer area. It temporarily holds data up to a certain limit. Enter a number to decide how many images to capture before a trigger is activated. Up to 7 images can be generated.

Send post-event images: Enter a number to decide how many images to capture after a trigger is activated. Up to 7 images can be generated.

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

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

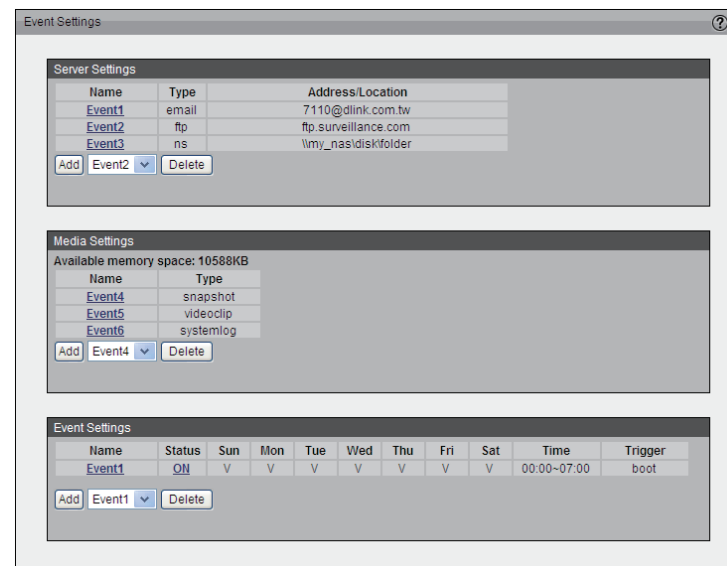
Click **Save** to enable the settings, then click **Close** to exit the page.

Video clip: Select to send video clips when a trigger is activated.

Source: Select a source of video clip.

Pre-event recording: The camera has a buffer area. It temporarily holds data up to a certain limit. Enter a number to decide the duration of recording before a trigger is activated. Up to 9 seconds can be set.

Maximum duration: Specify the maximum recording duration in seconds. Up to 20 seconds can be set. For example, if pre-event recording is set to 5 seconds and the



Configuration

maximum duration is set to 10 seconds, the camera continues to record for another 4 seconds after a trigger is activated.

Maximum file size: Specify the maximum file size allowed.

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

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

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

Click **Save** to enable the settings, then click **Close** to exit the page. When completed, click **Save** to enable the settings and click **Close** to exit this page. The new media settings will appear on the Event Settings page.

Event Settings

In the Event Settings column, click **Add** to open the Event Settings page. On this page, you can arrange three elements -- Trigger, Schedule, and Action to set an event. A total of 3 event settings can be configured.

Event name: Enter a name for the event.

Enable this event: Select to activate this event.

Priority: Set the priority for this event (High, Normal, or Low). The event with higher priority will be executed first

Detect next event after * seconds: Select the delay time before selecting the next event. It is being used for both events of motion detection and digital input trigger.

Trigger

This is the cause or stimulus which defines when to trigger the camera. The trigger source can be configured to use the camera's built-in motion detection mechanism or external digital input devices. There are several choices of trigger sources as shown below. Select the item to display the detailed configuration options. The input type that triggers the event.

Video motion detection: This option makes use of the built-in motion detection

The screenshot shows the 'Event Settings' interface with three main sections:

- Server Settings:** A table with columns 'Name', 'Type', and 'Address/Location'. It lists Event1 (email, 7110@dlink.com.tw), Event2 (ftp, ftp.surveillance.com), and Event3 (ns, \\my_nas\disk\folder). Below the table are 'Add', 'Event2' (dropdown), and 'Delete' buttons.
- Media Settings:** Shows 'Available memory space: 10588KB'. It has a table with columns 'Name' and 'Type', listing Event4 (snapshot), Event5 (videoclip), and Event6 (systemlog). Below are 'Add', 'Event4' (dropdown), and 'Delete' buttons.
- Event Settings Summary:** A table with columns: Name, Status, Sun, Mon, Tue, Wed, Thu, Fri, Sat, Time, Trigger. It shows Event1 with Status 'ON', a weekly schedule (V V V V V V V), Time '00:00-07:00', and Trigger 'boot'. Below are 'Add', 'Event1' (dropdown), and 'Delete' buttons.

Configuration

mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection for details.

Periodically: This option allows the camera to trigger periodically for every other defined minute. Up to 999 minutes are allowed.

Digital input: This option allows the camera to use an external digital input device or sensor as a trigger source. Depending on your application, there are many choices of digital input devices on the market which helps to detect changes in temperature, vibration, sound, and light, etc.

System boot: This option triggers the camera when the power to the camera is disconnected.

Recording notify: This option allows the camera to trigger when the recording disk is full or when recording starts to rewrite older data.

Camera tampering detection: This option allows the camera to trigger when the camera detects that it is being tampered with. To enable this function, you need to configure the Tamper detection option first. Please refer to Tamper detection for detailed information.

Event Schedule

Specify the period for the event

1. Select the days of the week.
2. Select the recording schedule in 24-hr time format.

Action

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

To set an event with recorded video or snapshots, it is necessary to configure the server and media setting so that the camera will know what action to take (i.e. the server to send the media files to) when a trigger is activated.

- **Add Server:** same as Server Settings
- **Add Media:** same as Media Settings

The screenshot shows a 'Recording' configuration window with the following settings:

- Recording name:** Record1
- Enable this recording
- Priority:** Normal
- Source:** Stream 1
- Trigger:** Schedule
- Recording Schedule:**
 - Sun Mon Tue Wed Thu Fri Sat
 - Time:**
 - Always
 - From 00:00 to 08:00 [hh:mm]
- Destination:** Event4
- Capacity:**
 - Entire free space
 - Reserved space: 100 Mbytes
- File name prefix:** [Empty text box]
- Enable cyclic recording

Buttons: Save, Close

Recording

Recording Settings

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

Recording name: Enter a name for the recording setting

Enable this recording: Select this option to enable video recording

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

Source: Select the recording source (stream 1 ~ 4).

Trigger: Select a trigger source.

Schedule: The server will start to record files on the network storage (NAS).

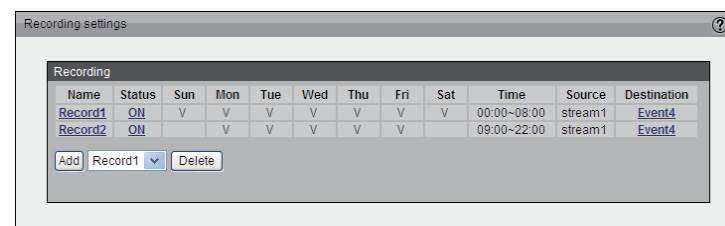
Recording Schedule: Specify the recording duration.

1. Select the days of the week.
2. Select the recording start and end times in 24-hr time format.

Destination: You can select the network storage that was set up for the recorded video files.

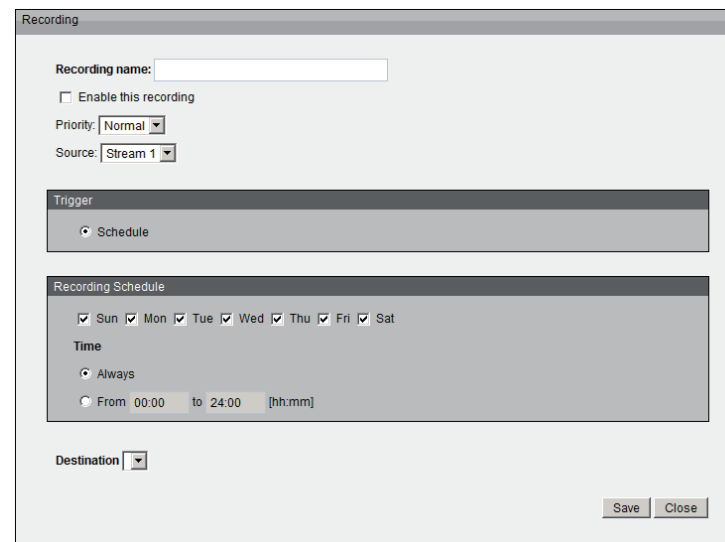
Capacity: You can choose either the entire free space available or limit the reserved space. The recording size limit must be larger than the reserved amount for cyclic recording.

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



Name	Status	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Source	Destination
Record1	ON	V	V	V	V	V	V	V	00:00-08:00	stream1	Event4
Record2	ON		V	V	V	V	V		09:00-22:00	stream1	Event4

Buttons: Add, Record1 (dropdown), Delete



Recording name:

Enable this recording

Priority:

Source:

Trigger

Schedule

Recording Schedule

Sun Mon Tue Wed Thu Fri Sat

Time

Always

From 00:00 to 24:00 [hh:mm]

Destination

Buttons: Save, Close

Configuration

Enable cyclic recording: If you select this item, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for cyclic recording to prevent malfunction. This value must be larger than 15 Mbytes.

If you want to enable recording notification, please click **Application** to set up. Please refer to Trigger > Recording notify for detailed information.

When completed, select Enable this recording. Click **Save** to enable the setting and click **Close** to exit this page. When the system begins recording, it will send the recorded files to the Network Storage.

The new recording name will appear in the drop-down list on the recording page.

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

PTZ Control

Digital PTZ

You can set a total of 20 preset positions and select preset positions for the camera to patrol.

Please follow the steps below to preset a position:

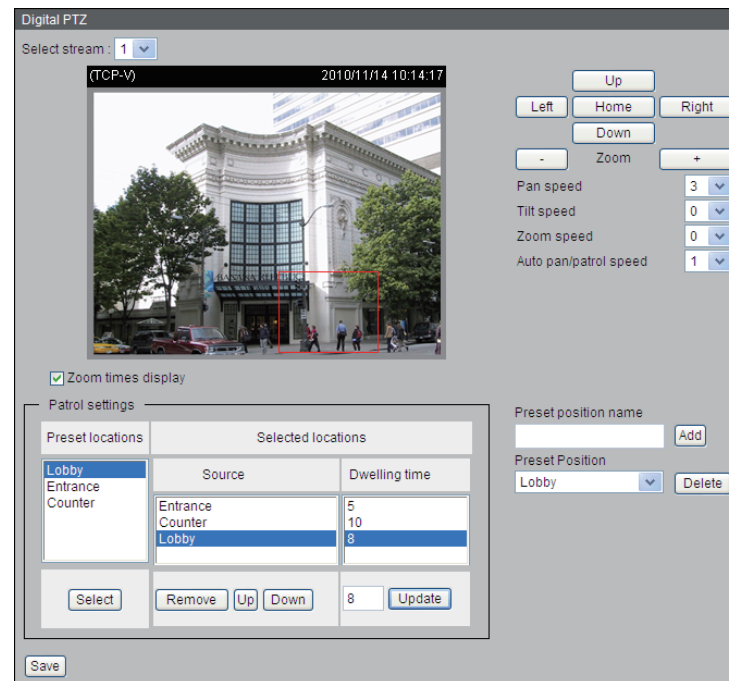
1. Adjust the shooting area to the desired position using the buttons on the right side of the window.
2. Enter a name for the preset position, which allows for up to forty characters. Click **Add** to enable the Setting. The preset positions will be displayed under the Preset Location list on the left-hand side.
3. To add additional preset positions, please repeat steps 1~2.
4. To remove a preset position from the list, select it from the drop-down list and click **Delete**.
5. The preset positions will also displayed on the main page. Please refer to the illustration on the next page.
6. Click **Save** to enable the setting. The Preset Positions will also be displayed on the Live Video. Select one from the drop-down list and the camera will move to the selected preset position.

Patrol Setting

You can select some preset positions for the camera to patrol.

Please follow the steps below to set up a patrol schedule:

1. Click a preset location on the list and click **Select**.
2. The selected preset location will be displayed on the Source list.
3. Set the Dwelling time for the preset location during auto patrol. You can also manually enter a value in the blank and click **Update**.
4. Repeat step 1 and 3 to select additional preset locations.
5. If you want to delete a selected location, select it from the Source list and click **Remove**.
6. Select a location and click **Up** or **Down** to rearrange the patrol order.
7. Click **Save** to enable the setting.



User Customization

Live Video Page Configuration

Preview: It shows the new layout of Logo/Background/Title based on user setting.

Logo Graphic: You can change the logo at the top of your Live Video page. Follow the steps below to upload a new logo:

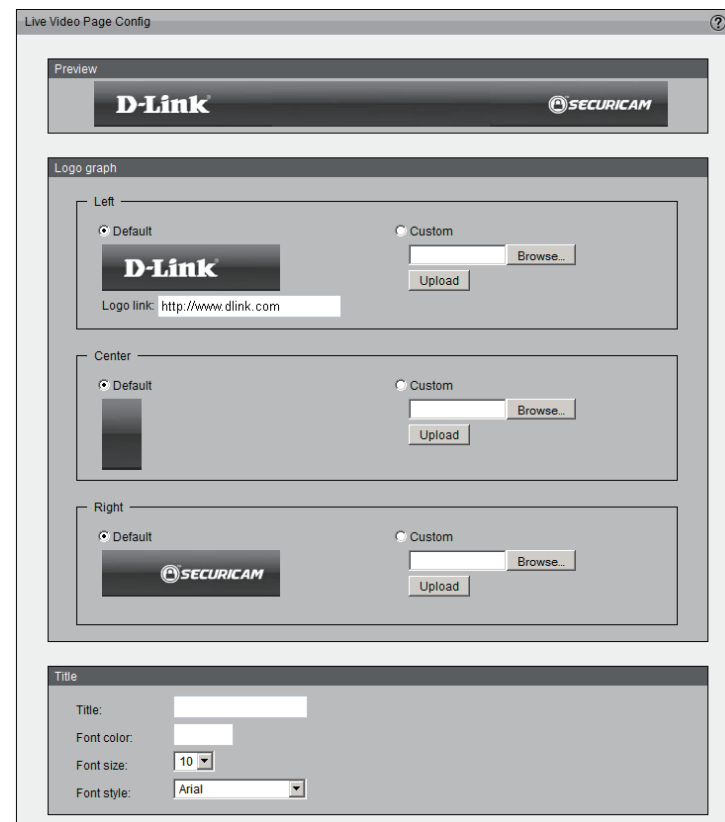
1. Click **Custom** and the Browse field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the setting.

Background: You can change the color of your Live Video page background. Follow the steps below to set up the customized Live Video page.

1. Click **Custom** on the left column.
2. Click the field where you want to change the color on the right column.
3. The palette window will pop up as shown below.
4. Drag the slider bar and click on the left square to select a desired color.
5. The selected color will be displayed in the corresponding fields and in the Preview column.

Click **Save** to enable the setting.

Title: You can also change the title at the top of your Live Video page.



HTML Code Examples

This page can generate example HTML code for you, thus you can paste the code into your own web page and get the embedded live video feed.

Stream:

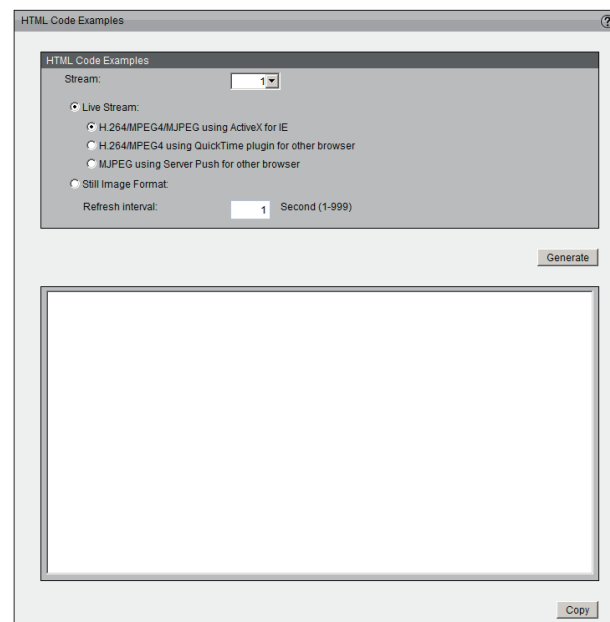
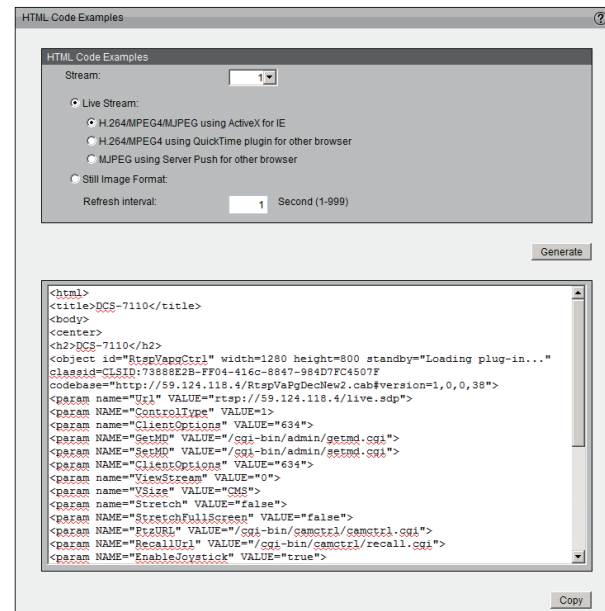
Select from stream 1 to 4, it will base on the profile of selected stream to generate the code accordingly. Up to 10 clients are supported for live view.

Live Stream:

- H.264/MPEG4/MJPEG using ActiveX for IE:**
 If target remote user client use Internet Explorer(IE), then the example code can support H.264, MPEG4 and MJPEG stream.
- H.264/MPEG4 using QuickTime plug-in for other browser**
 If target remote user client use QuickTime plug-in for the browser, then the example code can only support H.264 and MPEG4 stream.
- MJPEG using Server Push for other browser**
 If target remote user client use other browser, then the example code can only support MJPEG stream.

Still Image Format:

- Refresh interval second:**
 If user only need to embedded still image in the browser, please use this option and setup the refresh interval of the still image.



System User Settings

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

Admin Password Setup:

The administrator account name is "admin", which is permanent and cannot be deleted. The default of password is empty.

Add user account: Add a new user account.

Username: Enter a username for the new account.

Password: Enter a password for the new account.

Privilege: Select the access rights for the new user.

Manage user: Manage the accounts for existing users.

Authentication: The access rights for existing users.

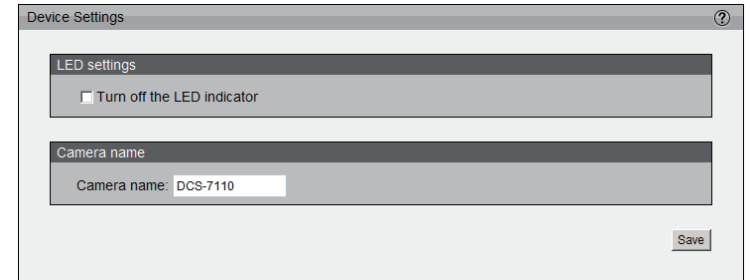
The screenshot displays the 'User Settings' web interface, which is organized into three main sections:

- Admin Password Setup:** This section contains two password input fields labeled 'Password:' and 'Retype password:', both filled with dots. A 'Save' button is located below the fields.
- Add User Account:** This section includes a 'User name:' field with the text 'Carlie', a 'Password:' field with dots, and a 'Confirm password:' field with dots. Below these is a 'Privilege:' section with three radio button options: 'Administrator', 'Normal user', and 'Guest'. An 'Add' button is positioned at the bottom of this section.
- Manage User:** This section features a 'User name:' dropdown menu currently set to 'User1', a 'User password:' field with dots, and an 'Authentication:' section with three radio button options: 'Administrator', 'Normal user', and 'Guest'. 'Modify' and 'Delete' buttons are located at the bottom.

Device Settings

Turn off the LED indicator: Select this option to turn off the LED next to the lens. This will prevent anyone from observing the operation of the network camera.

Camera Name: Create a unique name for your camera.



The screenshot shows a web browser window titled "Device Settings" with a help icon in the top right corner. The interface is divided into two main sections. The first section, titled "LED settings", contains a single checkbox labeled "Turn off the LED indicator", which is currently unchecked. The second section, titled "Camera name", contains a text input field labeled "Camera name:" with the value "DCS-7110" entered. A "Save" button is located in the bottom right corner of the form area.

Time and Date

Automatically or manually configure, update, and maintain the internal system clock for your camera.

Current Server Time: Displays camera's current time.

Time Zone: Select your time zone from the drop-down menu.

Enable Daylight Saving: Select this to enable the daylight saving time (DST). During DST, the system clock moves one hour ahead. (Note: To utilize this feature, be sure to first set the time zone of your network camera. Then starting and ending time of the DST is displayed upon selecting the option.)

Daylight Saving Dates: You may configure the daylight saving date and time.

Automatic Time Configuration: Enable this feature to obtain time configuration automatically from NTP server.

NTP Server: Network Time Protocol (NTP) synchronizes the network camera with an Internet time server. Choose the one that is closest to your location.

Update Interval: The time interval for updating the time information from NTP server.

Set the date and time manually: This option allows you to set the time and date manually.

Copy Your Computer's Time Setting: This will synchronize the time information from your PC.

The screenshot shows a 'Time and Date' configuration window with three main sections:

- Time Configuration:** Displays the current server time as '25 Oct 2010 15:18:46'. The time zone is set to 'GMT-05:00 Eastern Time, New York, Toronto'. There is an unchecked checkbox for 'Enable daylight saving'. Below, 'Daylight saving dates' are configured with 'DST start' on 'Jan 1st' at '12 am' and 'DST end' on 'Jan 1st' at '12 am'.
- Automatic time configuration:** Features radio buttons for 'Enable' and 'Disable'. The 'NTP server' field is empty, with a '<< Select NTP server' button. The 'Updating interval' is set to 'One hour'.
- Set the Date and Time manually:** Includes dropdown menus for Year (2010), Month (10), Day (25), Hour (15), Minute (18), and Second (46). A 'Copy Your Computer's Time Settings' button is present.

A 'Save' button is located at the bottom right of the window.

Maintenance

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

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

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

Restore to default: This feature allows you to restore the camera to factory default setting.

Export / Upload Files: This feature allows you to Export / Upload daylight saving time rules, custom language files, and setting backup files.

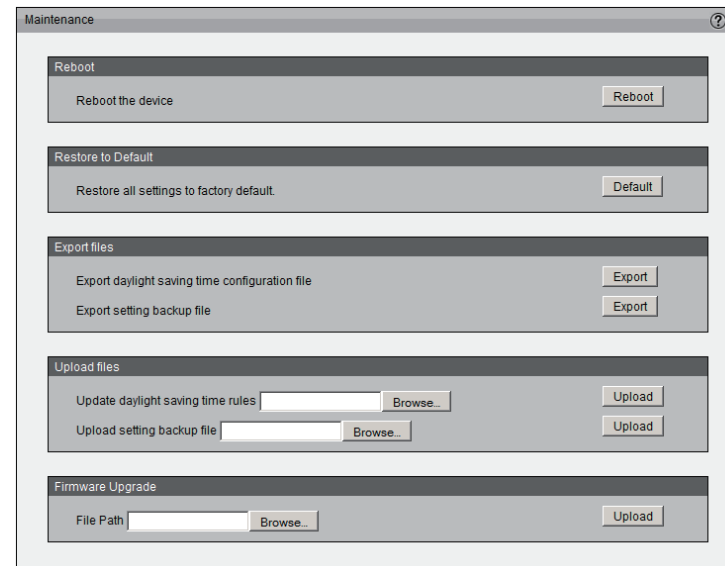
Export daylight saving time configuration file: Click to set the start and end time of DST.

Follow the steps below to export:

1. In the Export files column, click **Export** to export the daylight saving time configuration file from the camera.
2. A file download dialog will pop up as shown below. Click **Open** to review the XML file or click **Save** to store the file for editing.
3. Open the file with Microsoft® Notepad and locate your time zone. Set the start and end time of DST.
4. When completed, save the file

Upload daylight saving time rule: Click **Browse...** and specify the XML file to upload.

Export language file: Click to export language strings. DCS-7110 provides 5



languages: English, Deutsch, Español, Français, Italiano.

Upload custom language file: Click **Browse...** and specify your own custom language file to upload.

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

Upload setting backup file: Click **Browse...** to upload a setting backup file. Please note that the model and firmware version of the device should be the same as the setting backup file. If you have set up a fixed IP or other special settings for your device, it is not suggested to upload a settings backup file.

Firmware upgrade: This feature allows you to upgrade the firmware of your camera. It takes a few minutes to complete the process.

Note: Do not power off the camera during the upgrade!

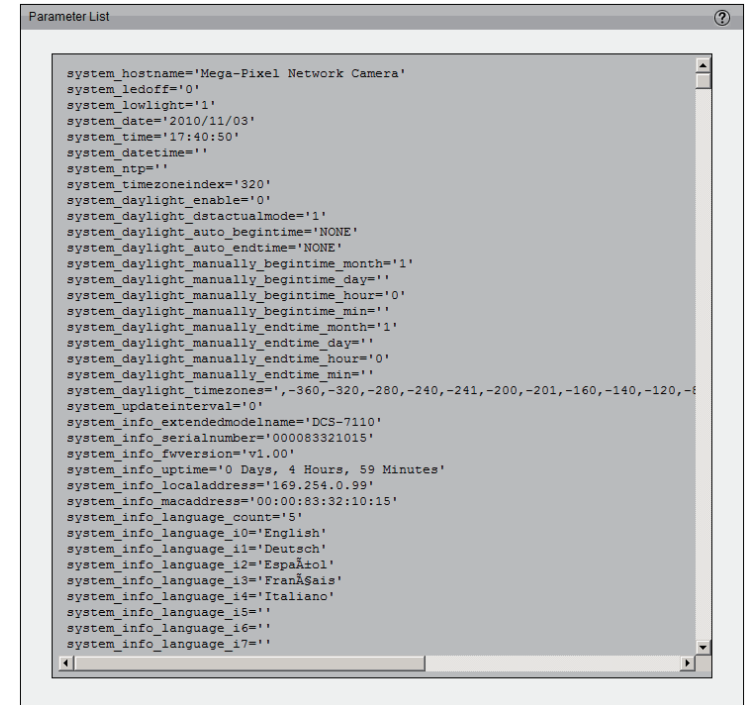
Follow the steps below to upgrade the firmware:

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

If the upgrade is successful, you will see "Reboot system now!! This connection will close". After that, re-access the camera.

Parameter List

The Parameters List page lists the entire system's parameters in alphabetical order. If you need technical assistance, please provide the information listed on this page.



```
system_hostname='Mega-Pixel Network Camera'  
system_ledoff='0'  
system_lowlight='1'  
system_date='2010/11/03'  
system_time='17:40:50'  
system_datetime=''  
system_ntp=''  
system_timezoneindex='320'  
system_daylight_enable='0'  
system_daylight_dstactualmode='1'  
system_daylight_auto_begintime='NONE'  
system_daylight_auto_endtime='NONE'  
system_daylight_manually_begintime_month='1'  
system_daylight_manually_begintime_day=''  
system_daylight_manually_begintime_hour='0'  
system_daylight_manually_begintime_min=''  
system_daylight_manually_endtime_month='1'  
system_daylight_manually_endtime_day=''  
system_daylight_manually_endtime_hour='0'  
system_daylight_manually_endtime_min=''  
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-160,-140,-120,-f'  
system_updateinterval='0'  
system_info_extendedmodelname='DCS-7110'  
system_info_serialnumber='000083321015'  
system_info_fwversion='v1.00'  
system_info_uptime='0 Days, 4 Hours, 59 Minutes'  
system_info_localaddress='169.254.0.99'  
system_info_macaddress='00:00:83:32:10:15'  
system_info_language_count='5'  
system_info_language_10='English'  
system_info_language_11='Deutsch'  
system_info_language_12='Español'  
system_info_language_13='Français'  
system_info_language_14='Italiano'  
system_info_language_15=''  
system_info_language_16=''  
system_info_language_17=''
```

Logs

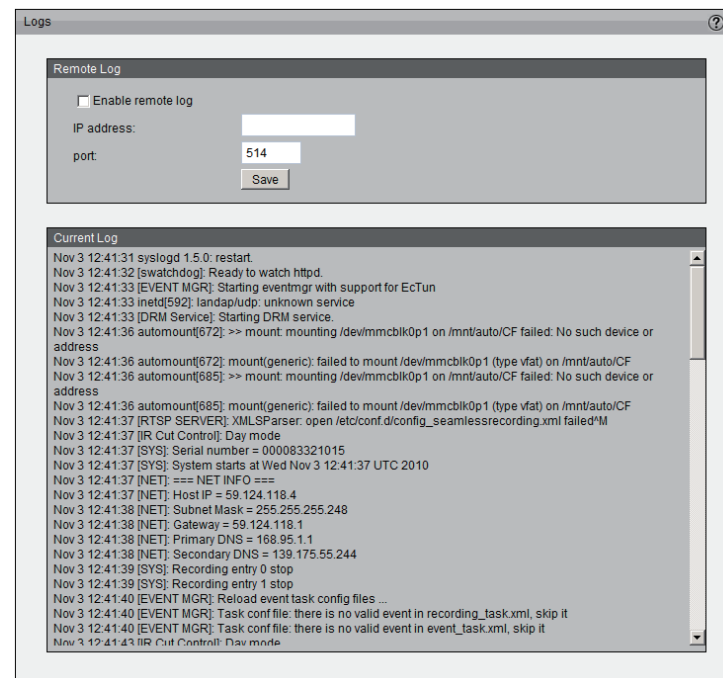
This section explains how to configure the camera to send the system log to the remote server as backup.

Remote Log: You can configure the camera to send the system log file to a remote server as a log backup. Before utilizing this feature, it is suggested that the a log-recording tool be first installed on the remote server to receive system log messages from the camera. Be sure to note the IP address of the remote server.

Follow the steps below to set up the remote log:

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

Current Log: This column displays the system log in chronological order. The system log is stored in the camera's buffer area and will be overwritten when reaching a certain limit.



Technical Specifications

Camera	Hardware Profile	<ul style="list-style-type: none"> ▪ 1/2.7" Megapixel progressive CMOS sensor ▪ 15 meter IR illumination distance ▪ Built-in Infrared-Cut Removable (ICR) Filter module ▪ Shutter Speed:1/5~1/25,000 	<ul style="list-style-type: none"> ▪ 4 mm fixed lens , F1.5 ▪ Minimum Object Distance: 0.4M ▪ Angle of view 77.4° (H) 45.1° (V) 88° (D)
	Image Features	<ul style="list-style-type: none"> ▪ Configurable image size, quality, frame rate, and bit rate ▪ Time stamp and text overlays ▪ 3 configurable motion detection windows ▪ Min Illumination: 0.12 Lux (day mode), 0 Lux (night mode) with IR LED 	<ul style="list-style-type: none"> ▪ 5 configurable privacy masks ▪ Flip & mirror ▪ Configurable white balance, shutter speed, brightness, saturation, contrast, sharpness
	Video Compression	<ul style="list-style-type: none"> ▪ H.264/MPEG4/MJPEG format compression simultaneously ▪ JPEG for still image 	<ul style="list-style-type: none"> ▪ H.264/MPEG-4 multicast streaming
	Video Resolution	1920x1080@15fps, 1600x904@20fps, 1360x768@25fps, 1280x800 @ 30 fps, 1280x720 @ 30 fps, 640x480 @ 30 fps, 320x240 @ 30 fps, 176x144 @ 30 fps,	
Network	Network Protocols	IPv4, IPv6, TCP/IP, UDP, ICMP, DHCP Client, NTP Client (D-Link), DNS Client, DDNS Client (D-Link), SMTP Client, FTP Client, HTTP / HTTPS, Samba Client, PPPoE, UPnP Port Forwarding, RTP / RTSP/ RTCP, IP filtering, 3GPP, LLTD, CoS/QoS, SNMP, IGMP, 802.1x, ONVIF Compliant	
	Security	<ul style="list-style-type: none"> ▪ Administrator and user group protection ▪ Password authentication ▪ HTTP and RTSP digest encryption 	<ul style="list-style-type: none"> ▪ HTTPS streaming ▪ Remote client access control
System Integration	System Requirements	<ul style="list-style-type: none"> ▪ Operating System: Microsoft Windows, 2000, XP, Vista, 7 ▪ Web Browser: Internet Explorer, 	
	D-ViewCam™ System Requirements	<ul style="list-style-type: none"> ▪ Operating System: Microsoft Windows 2003, XP, Vista, 7 ▪ Web Browser: Internet Explorer 7 or higher 	<ul style="list-style-type: none"> ▪ Protocol: Standard TCP/IP
	Event Management	<ul style="list-style-type: none"> ▪ Motion detection ▪ Event notification and upload snapshots/video clips via HTTP, SMTP or FTP ▪ Supports multiple HTTP, SMTP and FTP servers 	<ul style="list-style-type: none"> ▪ Multiple event notification ▪ Multiple recording methods for easy backup
	Remote Management	<ul style="list-style-type: none"> ▪ Configuration accessible via web browser ▪ Take snapshots/video clips and save to local hard drive 	
	Surveillance Software Function	<ul style="list-style-type: none"> ▪ Remote management/control of up to 32 cameras ▪ Viewing of up to 32 cameras on one screen 	<ul style="list-style-type: none"> ▪ Supports all management functions provided in web interface ▪ Scheduled motion triggered, or manual recording options
	External Device Interface	<ul style="list-style-type: none"> ▪ DI and DO for external sensor and alarm 	

Appendix A - Technical Specifications

General	Power Input	12 V DC 1.25 A, 24 V AC, 50/60 Hz, 802.3af PoE
	Max. Power Consumption	6.3 W
	Operating Temperature	-20 to 50 °C (-4 to 122 °F)
	Storage Temperature	-20 to 70 °C (-4 to 158 °F)
	Humidity	90% non-condensing
	Weight	808 g
	Certifications	CE (Class A), LVD, FCC (Class A), C-Tick
Dimensions	<p>The technical drawing consists of two views of the device. The top view on the left shows a circular face with a diameter of 72.94 mm and a central circular feature with a diameter of 66.00 mm. The side view on the right shows the device's profile with a total length of 197.19 mm, a base length of 178.54 mm, and a height of 70.50 mm.</p>	