



User Manual

DCS-3511 HD PoE Network Camera DCS-3530 HD Wireless Network Camera

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
1.0	August 06, 2013	DCS-3511/DCS-3530 Revision A1 with firmware version 1.00
1.1	September 09, 2014	add RF Warranty Sentence

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 © 2014 by D-Link Corporation.

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

Table of Contents

Product Overview	5	Audio Settings	36
Package Contents.....	5	Day and Night Settings.....	37
System Requirements	6	Network.....	38
Introduction	7	IP Settings.....	38
Features.....	8	Wireless Settings	40
Hardware Overview.....	9	Port and Access Name Settings.....	41
Front Panel	9	Dynamic DNS	44
Rear Panel.....	10	HTTPS.....	45
Side Panel	11	Access List.....	47
Button Panel	12	Advanced Settings	49
Installation	13	Event Management	53
Hardware Installation.....	13	Motion Detection	53
Configuration with Wizard	14	Tamper Detection.....	54
Viewing Camera via Web Browser	19	DI and DO	55
D-ViewCam Setup Wizard.....	21	Event Settings	56
Configuration	23	Recording	62
Live Video	23	Recording Settings.....	62
Client Setup	27	Local Storage.....	64
Setup.....	28	PTZ Control	65
Standard Setup.....	28	Digital PTZ.....	65
Advanced Setup.....	29	Mechanical PTZ	66
System Overview	30	System	67
Video	31	User Settings	67
Video Settings.....	31	Device Settings.....	68
Image Settings.....	34	Time and Date.....	69
		Maintenance.....	70

Parameter List	72
Logs	73
Appendix A - Technical Specifications.....	74
Technical Specifications	74

Package Contents



DCS-3511 DCS-3530
HD Network Camera



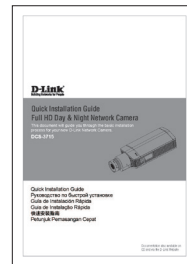
Mounting Bracket



**User Manual and Software on
CD-ROM**



Power Adapter



Quick Install Guide



CAT5 Ethernet Cable



Accessory
**Wrench, lens ring fixture,
I/O connectors**



Antenna
(DCS-3530 only)



Video 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 7 or higher, Firefox, Chrome, Safari
- 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

DCS-3511/3530 are HD, full frame rate network camera with H.264 compression. The DCS-3511/3530 connect to a network to provide high-quality live video over the Internet. With the vivid video quality and superb high resolution, it can provide most detail of the video which is useful to identify any suspected object. DCS-3511/3530 provide multiple streaming and flexible viewing window settings for different purpose of surveillance, either for regular recording or mobile view. Built-in microSD card slot can record important events in microSD card as a local backup and it's very easy to retrieve.

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

HD Surveillance

DCS-3511/3530 provide HD industrial standard 16:9 wide screen video for IP surveillance. With the vari-focal lens, it is a high performance high quality network camera. To utilize the advantage of high resolution, the "viewing window" design can provide user a flexible settings to monitor multiple ROI (Region of Interest) by a single camera. And the "ePTZ" can also simulate wide area surveillance by digital zoom and pan, tilt control.

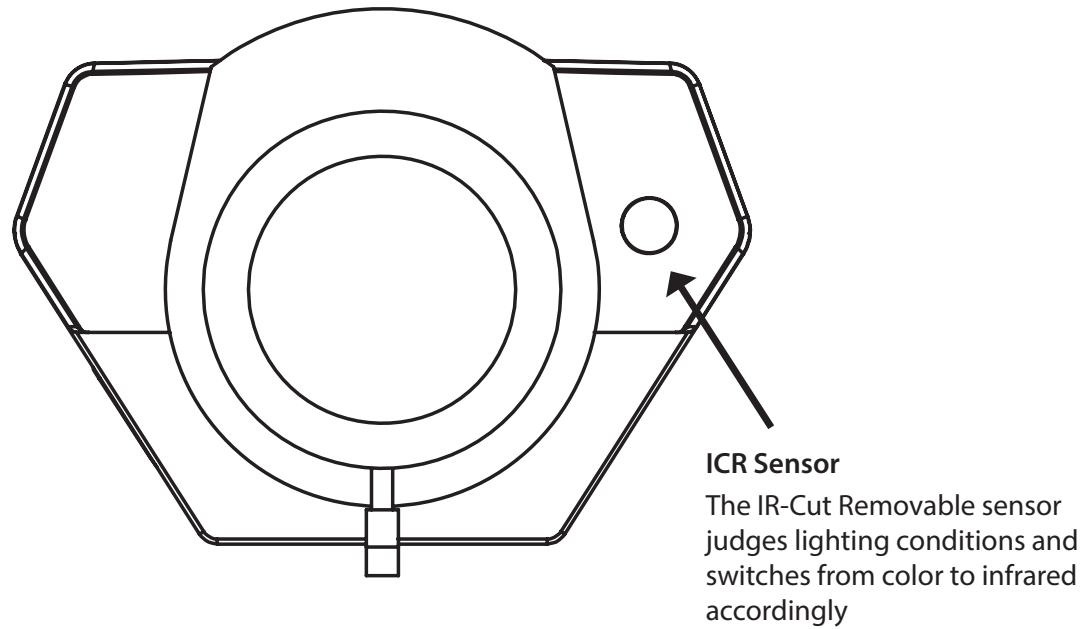
Flexible Connectivity

The DCS-3511 incorporates Power over Ethernet (PoE), allowing it to be easily installed in a variety of locations without the need for supplemental power cabling.

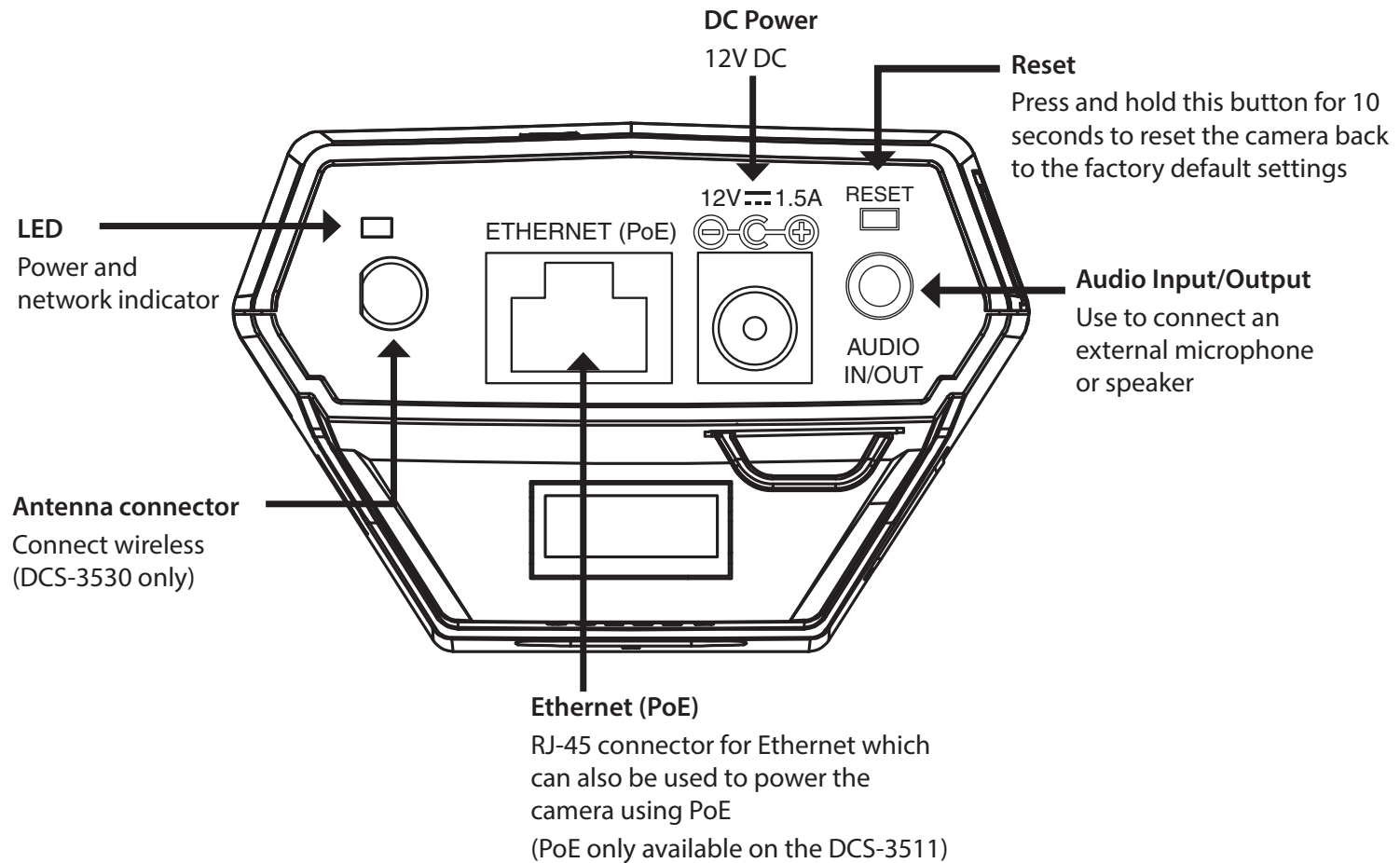
The DCS-3530 works with a 10Mbps Ethernet based network or 100Mbps Fast Ethernet based network for traditional wired environments, and works with 802.11n routers or access points for added flexibility.

Hardware Overview

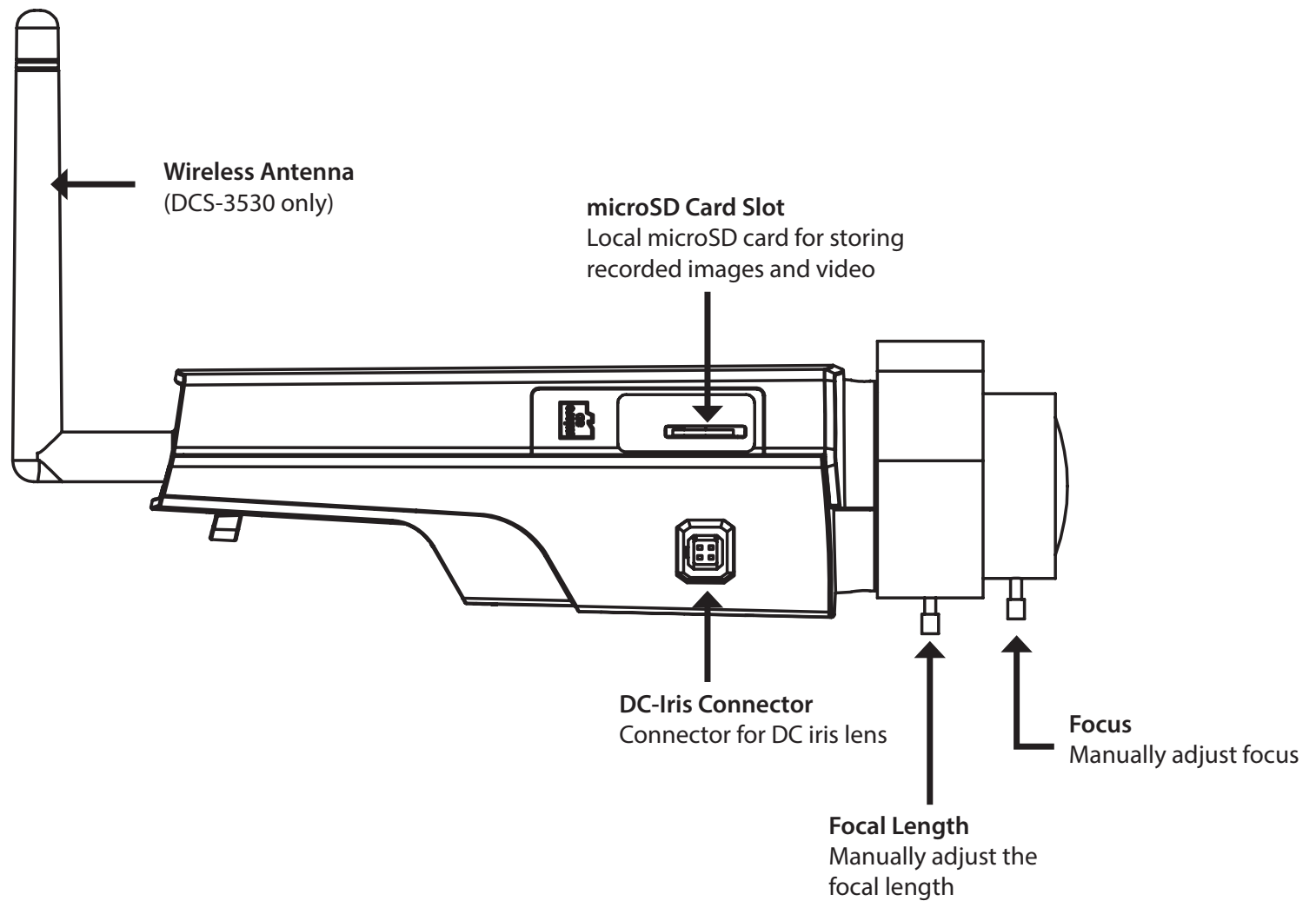
Front Panel



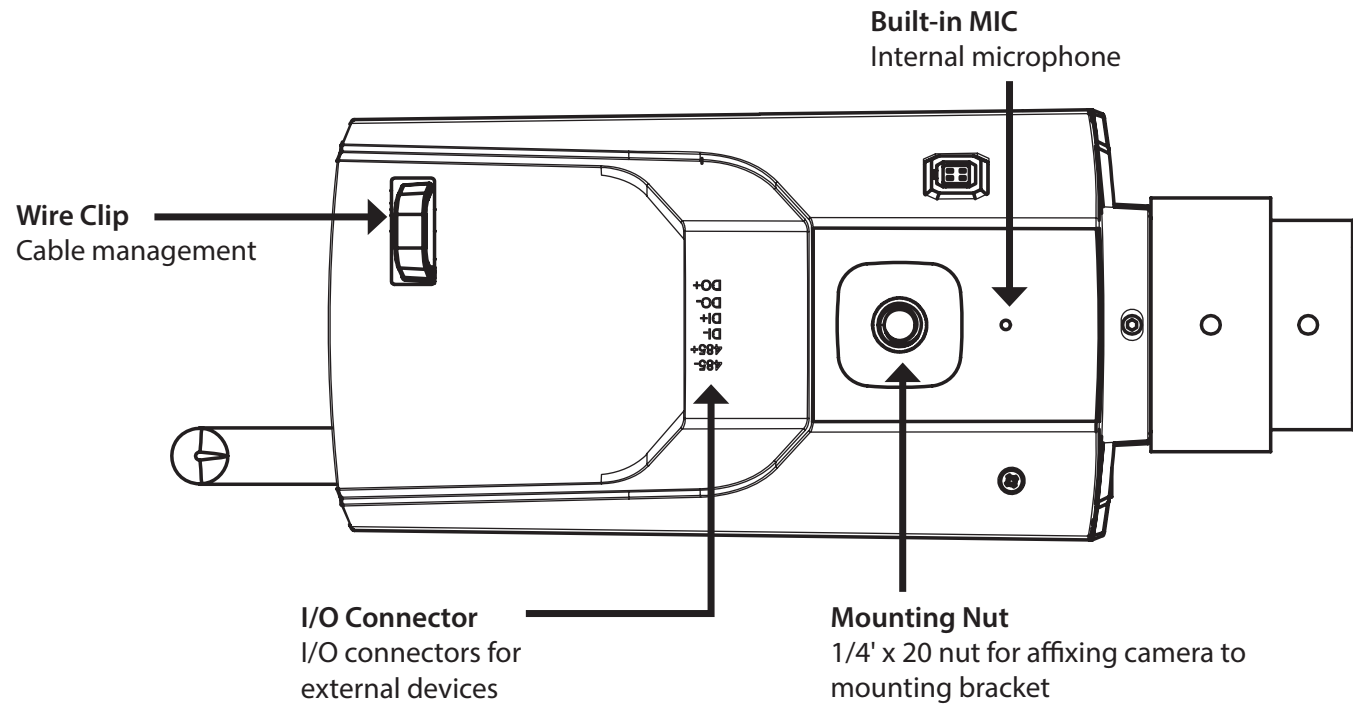
Rear Panel



Side Panel



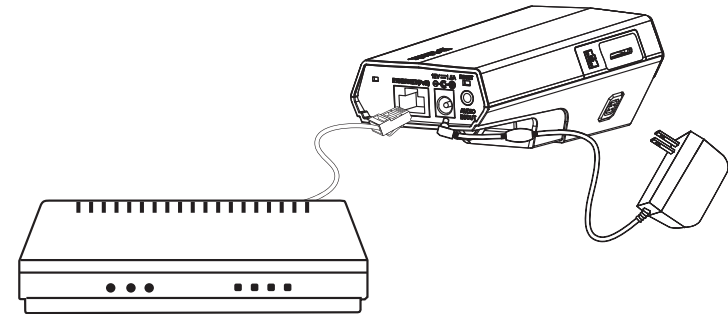
Button Panel



Hardware Installation

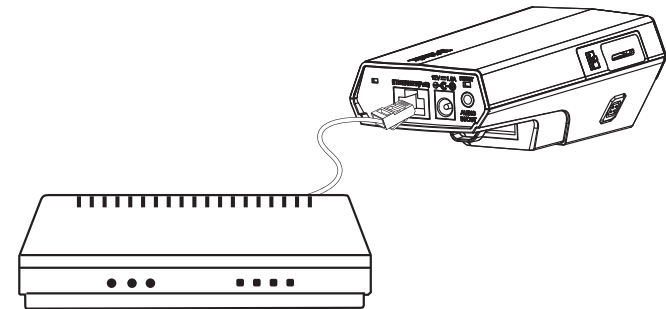
Basic Connection (without PoE)

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



Connection Using a PoE Switch

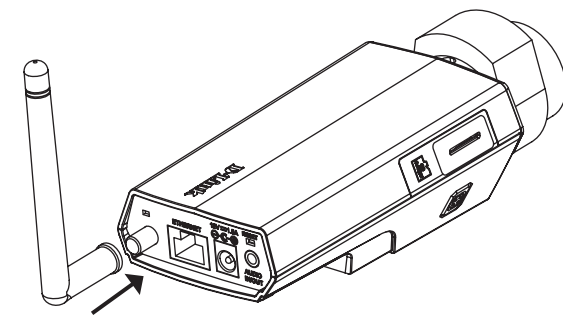
If using a PoE switch or router, connect the network camera via Ethernet cable.
PoE will transmit both power and data over a single cable.



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.

Attach the Antennas (DCS-3530 only)

Locate the antenna included with your DCS-3530 and attach it to the antenna connector located on the back of the DCS-3530.



Configuration with Wizard

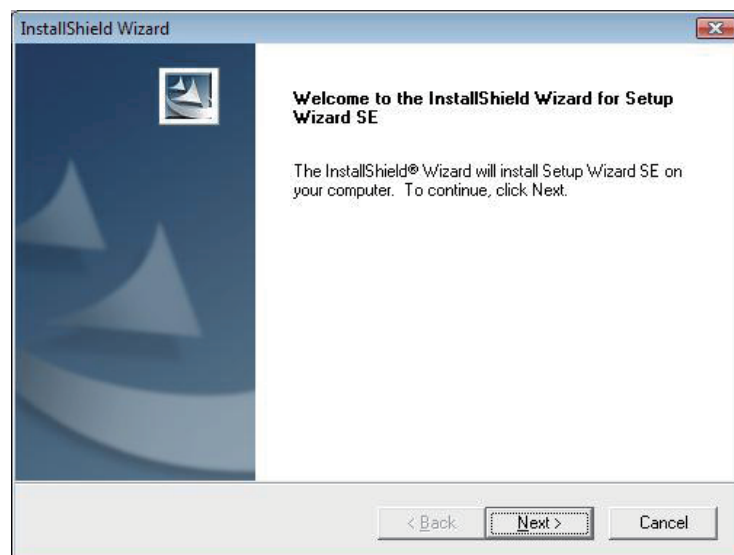
Insert the DCS-3511/DCS-3530 CD into your computer's CD-ROM drive to begin the installation. If the Autorun function on your computer is disabled, or if the D-Link Launcher fails to start automatically, click **Start > Run**. Type **D:\autorun.exe**, where D: represents the drive letter of your CD-ROM drive.

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

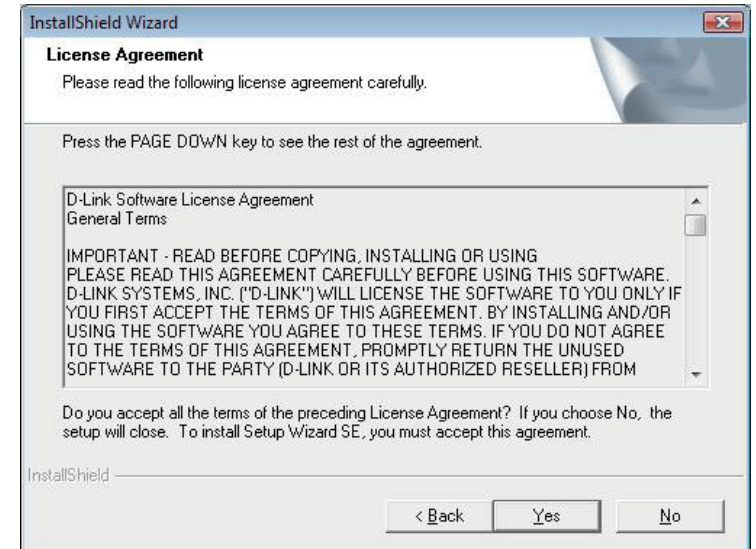


After clicking Setup Wizard, the following window will open.

Click **Next** to continue.

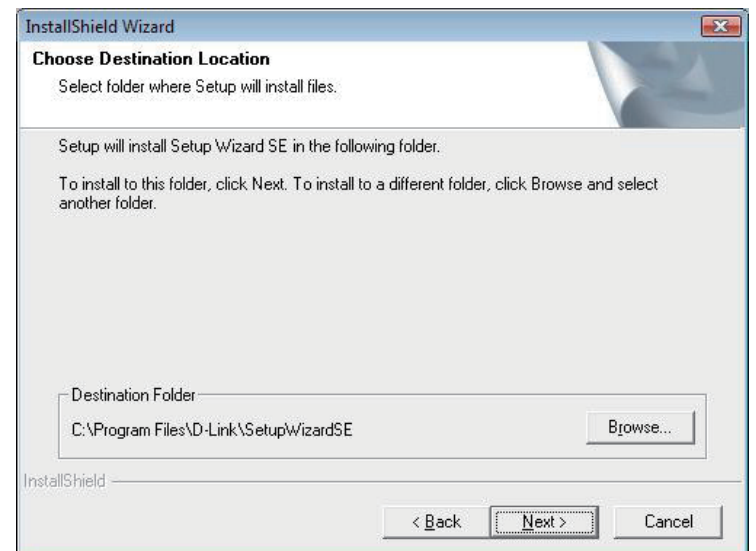


Click **Yes** to accept the License Agreement.

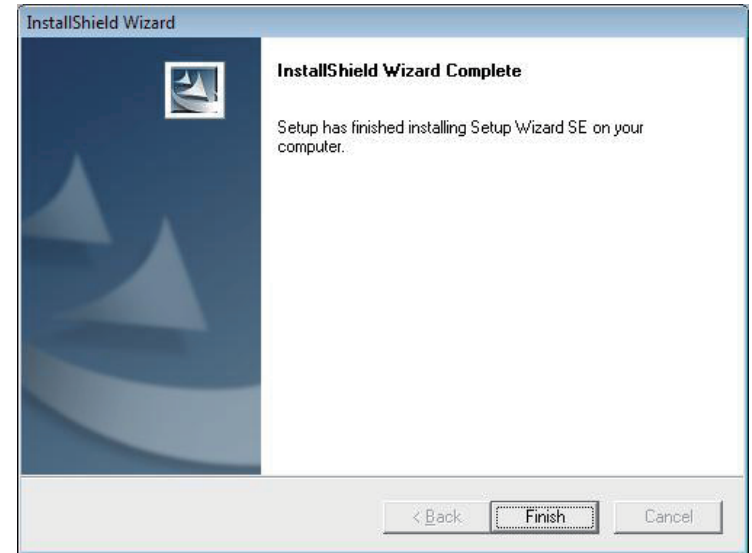


To start the installation process, click **Next**.

Note: The installation may take several minutes to finish.

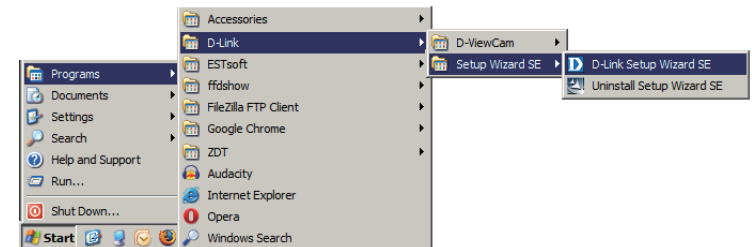


Click **Finish** to complete the installation.



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

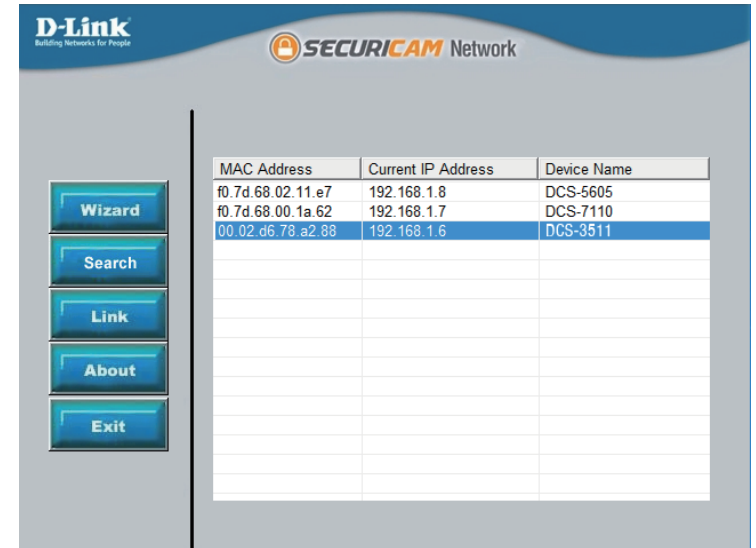
Start > D-Link > Setup Wizard SE



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 **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.



Installation

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.



The screenshot shows the 'Set IP Address' configuration page in the D-Link SecurICAM Network web interface. The page has a blue header with the D-Link logo and 'SECURICAM Network' text. The main content area is light gray and contains the following settings:

- DHCP
- Static IP
- IP Address: 192.168.1.185
- Subnet Mask: 255.255.255.0
- Default Gateway: 192.168.1.1
- Primary DNS: 192.168.1.1
- Secondary DNS: 192.168.1.1

At the bottom right, there are three buttons: 'Back' (left arrow), 'Next' (right arrow), and 'Exit' (power icon).

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



The screenshot shows the configuration page after the IP address settings have been confirmed. The 'Static IP' option is now selected. The settings are:

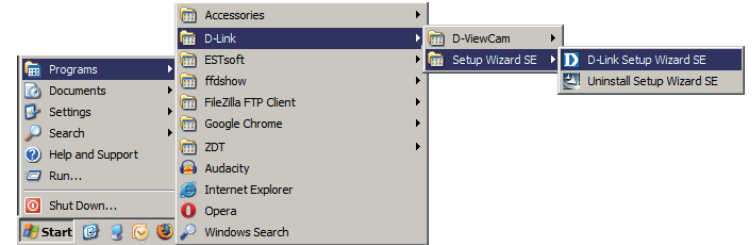
- Admin ID: admin
- Password: (empty field)
- IP Address: 192.168.0.102
- Subnet Mask: 255.255.255.0
- Primary DNS: 192.168.0.1
- Secondary DNS: 192.168.0.1

Below the settings, a message reads: "The Setup Wizard has completed. Click on 'Back' to modify your settings. Click 'Restart' to save your current settings and reboot the Internet Camera." At the bottom right, there are two buttons: 'Back' (left arrow) and 'Restart' (refresh/circular arrow icon).

Viewing Camera via Web Browser

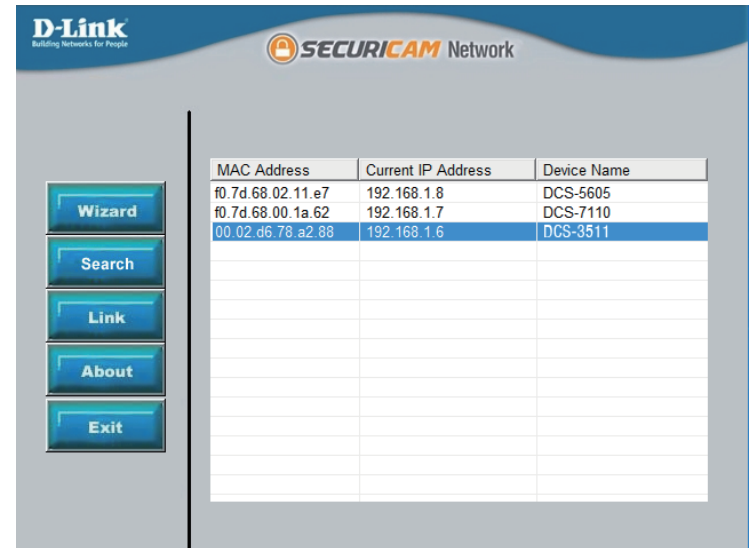
Click on the **D-Link Setup Wizard SE** icon that was created in your Windows Start menu.

Start > D-Link > Setup Wizard SE



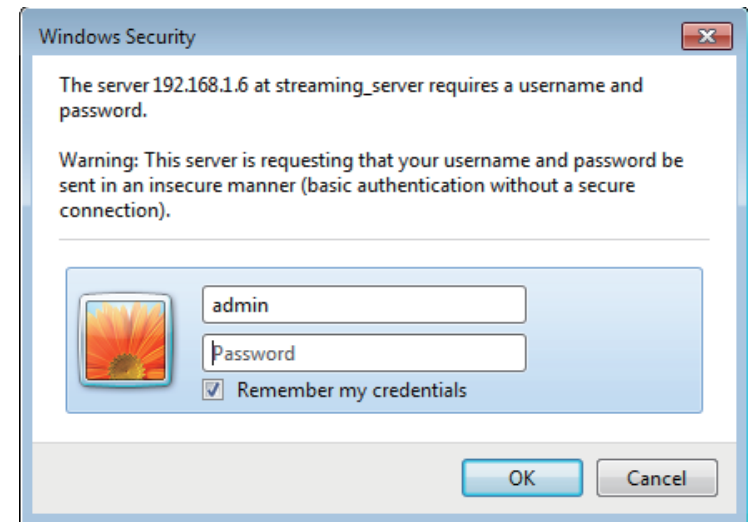
Select the camera and click the button labeled **"Link"** to access the web configuration.

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

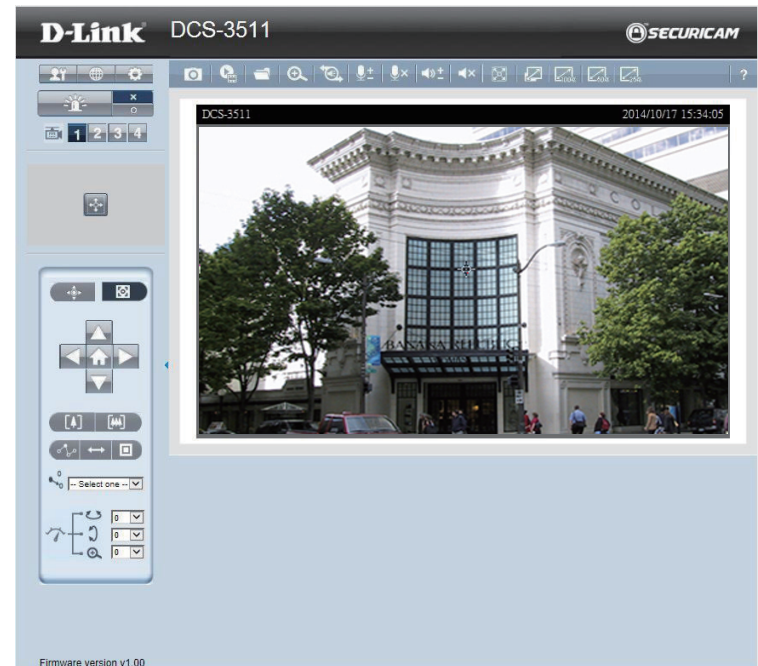


Installation

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.



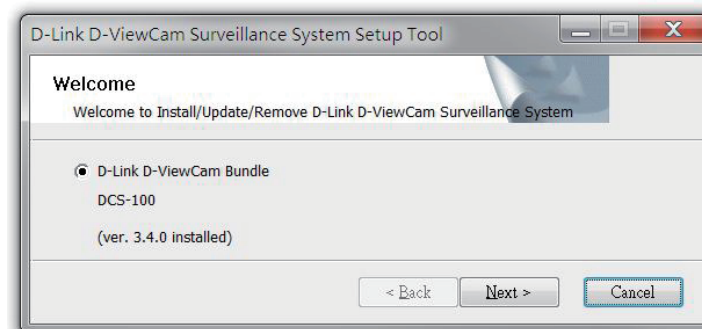
D-ViewCam Setup Wizard

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. A menu screen will appear as shown below.

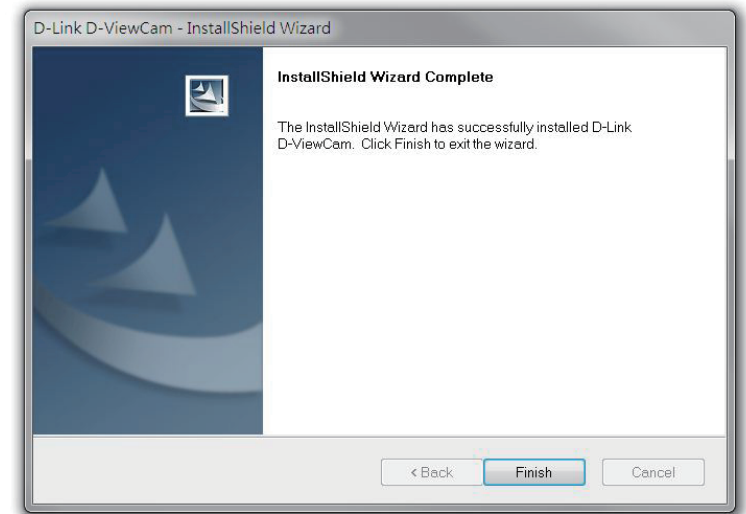


Follow the Installation Wizard to install D-ViewCam.

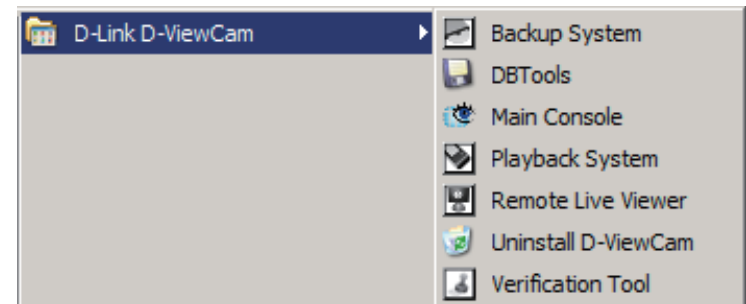


Installation

Click **Finish** to complete the installation.



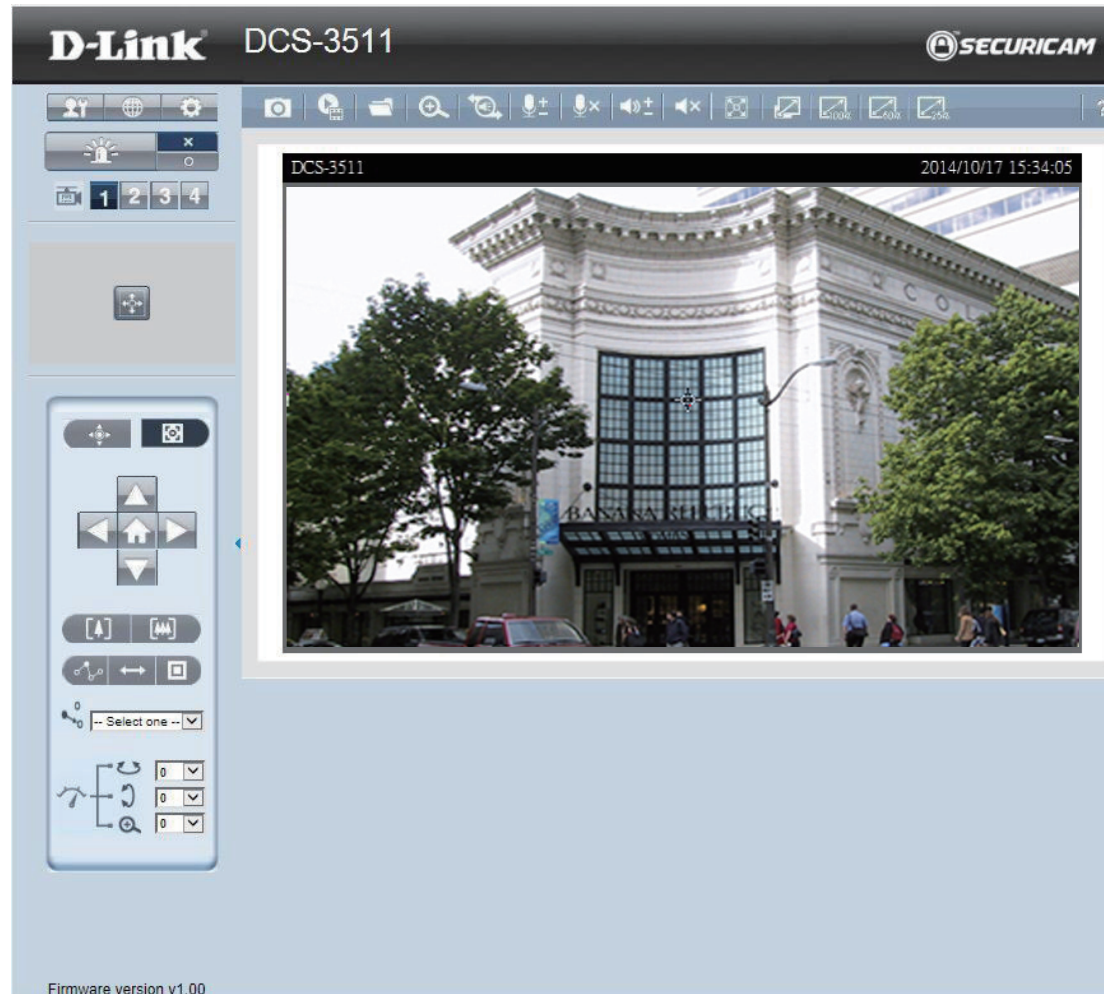
To start D-ViewCam, select **Start > All Programs > D-Link D-ViewCam > Main Console**.











For more information about D-ViewCam, please refer to the documentation on the D-ViewCam CD-ROM.















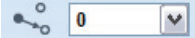
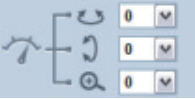



Live Video

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.

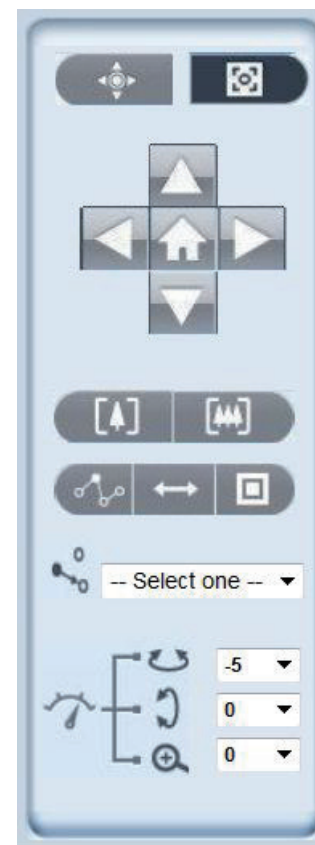


	<p>Click this logo to visit the D-Link website. The logos and website can be customized to fit your needs. For more information, please refer to User Customization on page 68.</p>
	
 <p>Client Settings</p>	<p>Setup the stream transmission mode and saving options on the local computer.</p>
 <p>Language</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 31.</p>

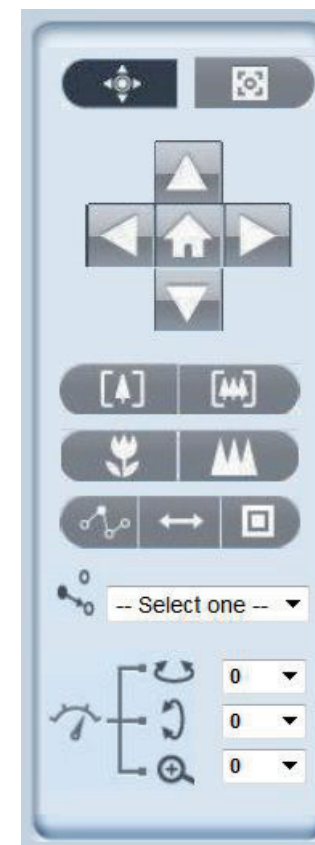


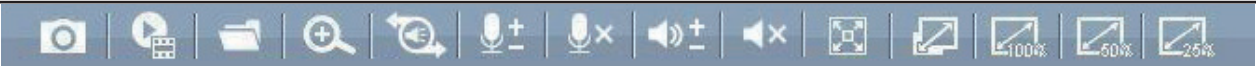












 <p>PTZ Control</p>	<p>This camera supports both “digital” (e-PTZ) and “mechanical” pan/tilt/zoom control. Please refer to PTZ Control for detailed information.</p> <p> Mechanical PTZ: Connect the camera to a PTZ driver or scanner via RS-485 interface.</p> <p> Digital PTZ: Control the e-PTZ operation. It allows users to quickly move the focus to a target area for close-up viewing without physically moving the camera.</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>Focus</p>	<p>Control camera focus to get a clear image. (Available only under mechanical PTZ mode*)</p> <p> Focus Near  Focus Far</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: 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 or 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>

Digital PTZ Control Panel




Mechanical PTZ Control Panel



<h1>Camera Control</h1> 	
 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>
 Two way audio	<p>Click this button to talk to people around the Network Camera if there is an external speaker connected to the camera and you have a microphone connected to your computer. Press the icon again to stop talking or disable this function.</p>
 Microphone Level	<p>Microphone Level: When the mute function is not active, move the slider bar to adjust the level of the microphone (internal/external) that is connected to your network camera.</p>
 Microphone Mute	<p>Microphone Mute/Un-mute: Click to turn off the microphone (internal/external) that is connected to your network camera. Press again to turn the microphone back on.</p>
 Speaker Volume	<p>Speaker Volume - When the mute function is not active, move the slider bar to adjust the volume of the speakers that are connected to your network camera.</p>
 Speaker Mute	<p>Speaker Mute/Un-mute: Click to mute the external speaker that is connected to the network camera. Press again to un-mute the speaker.</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 Media Options

Video and Audio can be viewed at the same time or separately.

Recording Options

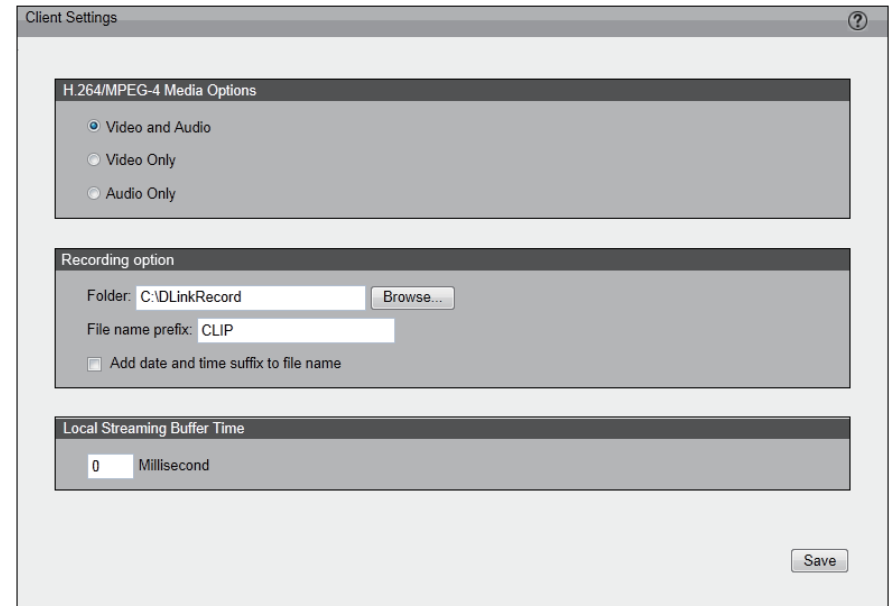
Folder: Select the folder where you would like the recording file saved on your desktop computer.

File name prefix: Enter a file name prefix for the recording 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 Media Options:** Three radio buttons are present: 'Video and Audio' (selected), 'Video Only', and 'Audio Only'.
- Recording option:** A 'Folder:' label is followed by a text box containing 'C:\DLinkRecord' and a 'Browse...' button. Below it, 'File name prefix:' is followed by a text box containing 'CLIP'. A checkbox labeled 'Add date and time suffix to file name' is currently unchecked.
- Local Streaming Buffer Time:** A text box contains the number '0', followed by the label 'Millisecond'.

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

Setup

The DCS-3511/DCS-3530 includes standard and advanced setup screens. Both screens include a tree view with multiple setup options. This manual includes detailed explanations for all advanced setup screens.

Standard Setup

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

Click on the **standard** 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

Audio and Video

- Video Settings, Audio Settings, Day and Night Settings

Network

- IP Settings, *Wireless Settings.

Event Management

- Motion Detection, Tamper Detection, DI and DO

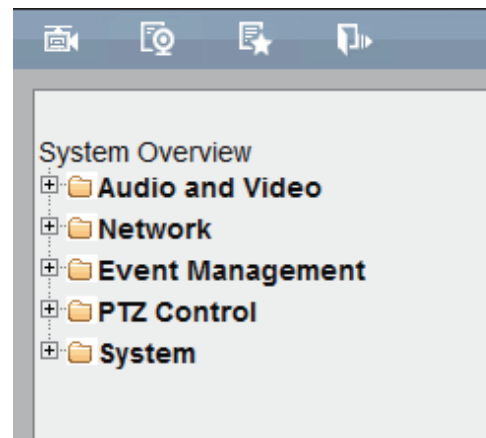
PTZ Control

- Digital PTZ, Mechanical PTZ.

System

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

*Function for DCS-3530 only.



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

Audio and Video

- Video Settings, Image Settings, Audio Settings, Day and Night Settings

Network

- IP Settings, *Wireless 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, Local Storage

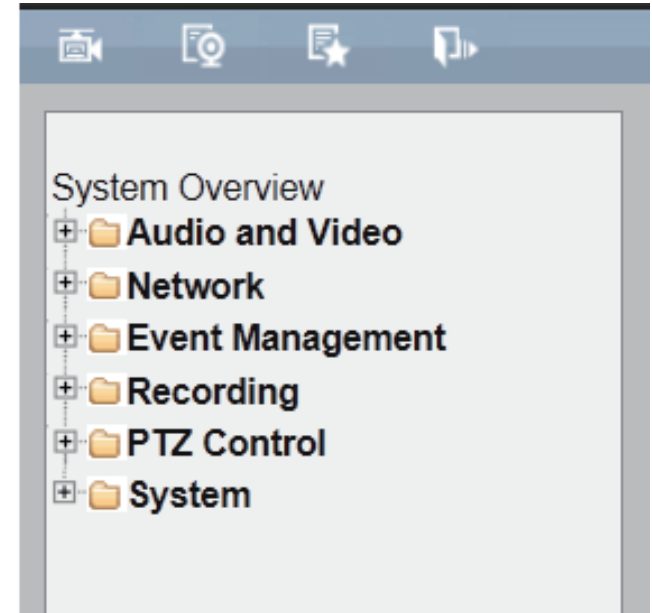
PTZ Control

- Digital PTZ, Mechanical PTZ

System

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

*Function for DCS-3530 only.



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.

D-Link DCS-3511 **SECURICAM**

192.168.1.6

System Overview

Device Information

IP address	192.168.1.6
Link-local address	169.254.0.99
Current firmware version	v1.00
Current firmware date	28 Apr 2011
MAC address	10.A9.55.66.77.89
Connect client	1

Time and Date

Current system time	23 Jan 2000 22:15:25
System up time	0 Days, 2 Hours, 8 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	1920x1080	30	Excellent
Stream 2	H.264	1280x720	30	3 Mbps
Stream 3	H.264	176x144	5	40 kbps
Stream 4	H.264	1920x1080	30	3 Mbps

Recent Logs

```

Jan 23 21:07:31 udhccp: router 192.168.1.1
Jan 23 21:07:32 udhccp: dns 192.168.1.1
Jan 23 21:18:32 [IR Cut Control]: Night mode
Jan 23 21:37:33 udhccp: IP 192.168.1.6 netmask 255.255.255.0
Jan 23 21:37:33 udhccp: router 192.168.1.1
Jan 23 21:37:33 udhccp: dns 192.168.1.1
Jan 23 22:07:34 udhccp: IP 192.168.1.6 netmask 255.255.255.0
Jan 23 22:07:34 udhccp: router 192.168.1.1
Jan 23 22:07:34 udhccp: dns 192.168.1.1
Jan 23 22:07:50 [IR Cut Control]: Day mode
    
```

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 176x144 to 1280x800. 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:

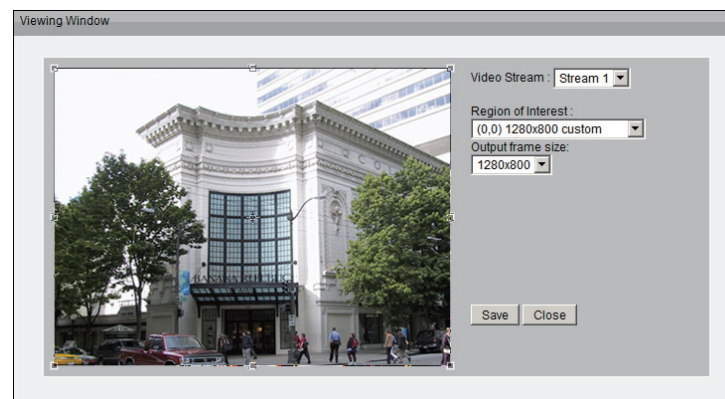
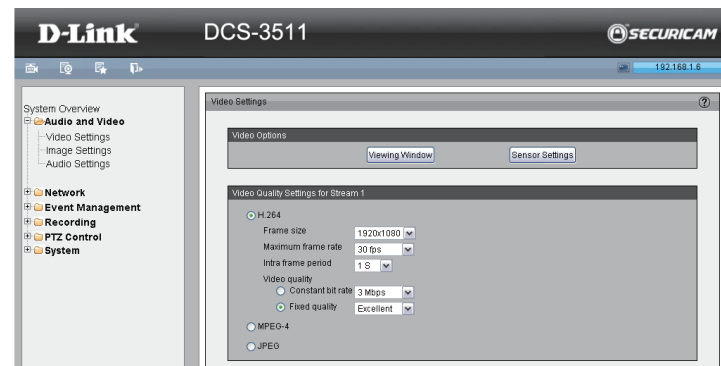
1. Select a stream whose viewing region you would like to set.
2. Select a Region of Interest from the drop-down list, the floating frame will resize accordingly. If you want to set up a customized viewing region, you can also resize and drag the floating frame to a desired position with your mouse.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

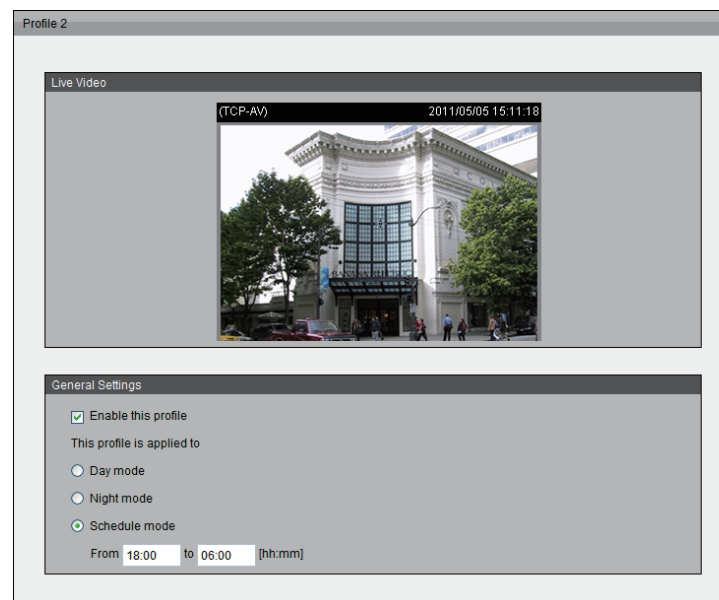
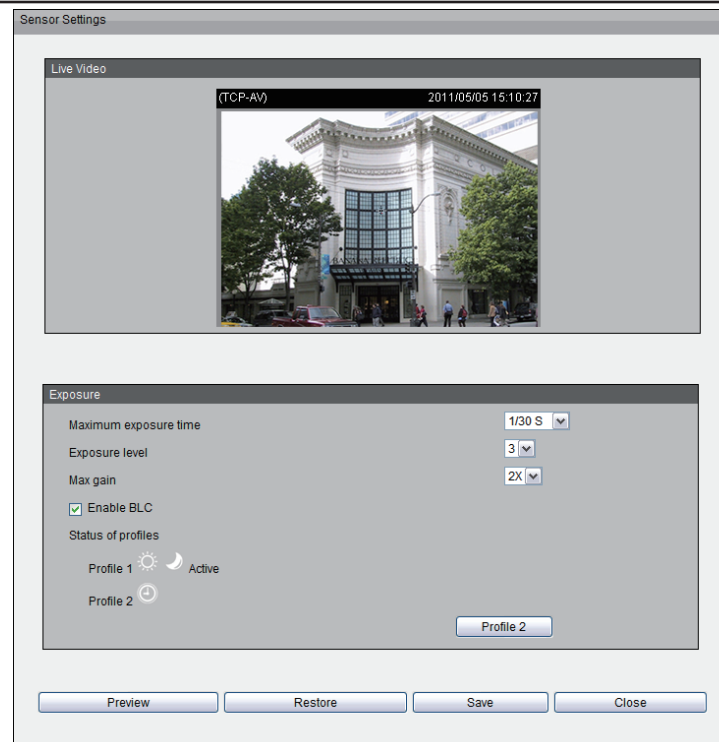
Sensor Setting: Click **Sensor Setting** to open the Sensor Setting page. On this page, you can set the maximum exposure time, exposure level, and AGC (Auto Gain Control) setting. You can configure two sets of sensor setting: one for normal situations(Profile 1), the other for special situations, such as day/night/schedule mode(Profile 2).

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: 1/5,1/15,1/30,1/60,1/120.
- **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, 8x, 16x, 32x). 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 Configure Image setting in the third 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 13 options you can select: from 1280x800 to 176x144.

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, 2, 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 6 Mbps.
- **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.

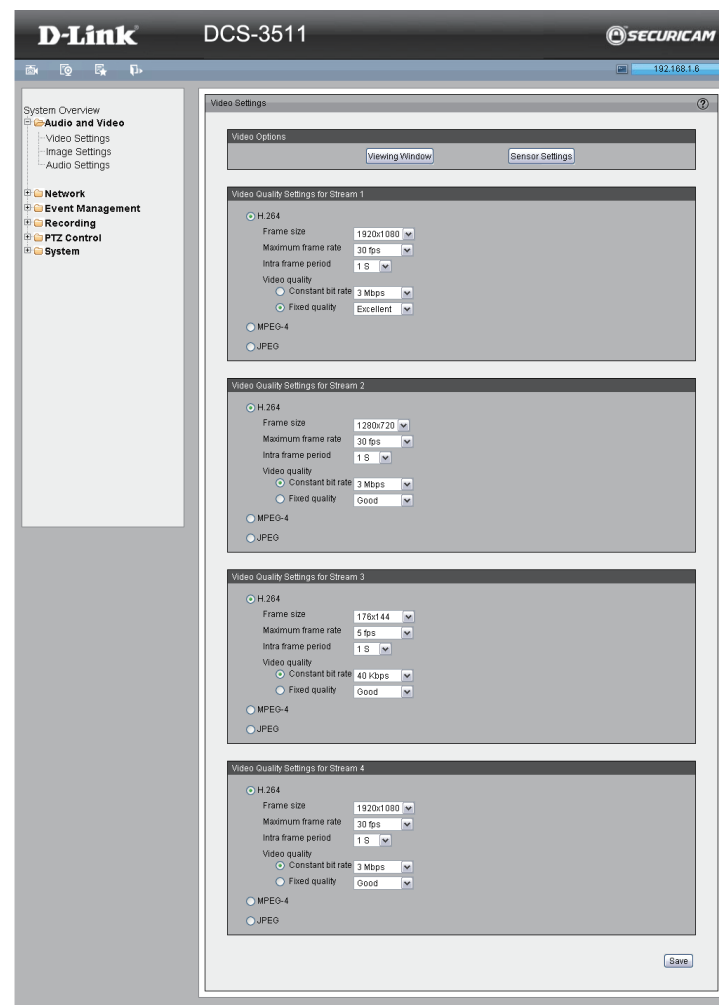


Image Settings

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.

Iris mode: fixed, indoor, outdoor

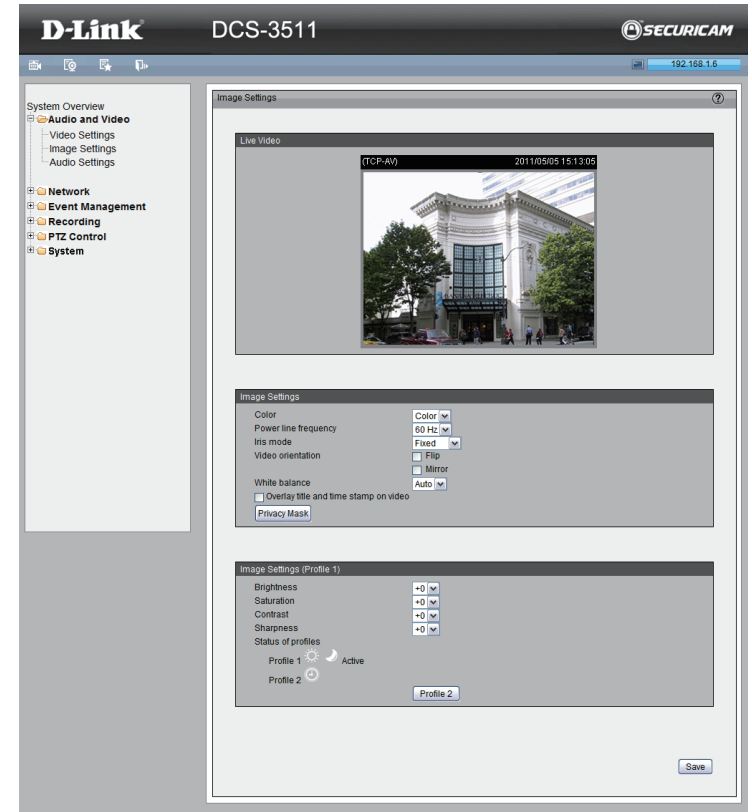
Video Orientation: Flip will vertically rotate the video. Mirror will horizontally rotate the video. You may select both options if camera is being installed upside down.

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.)

Note:

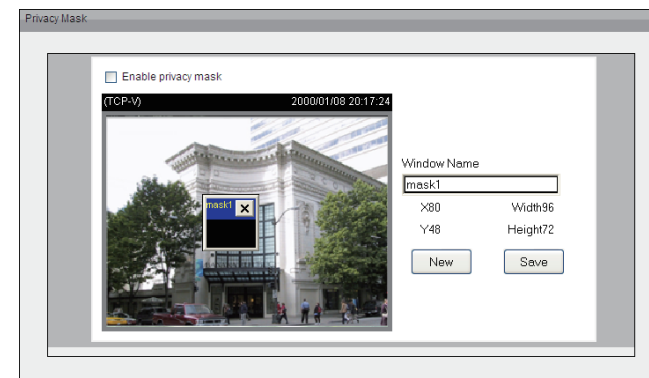
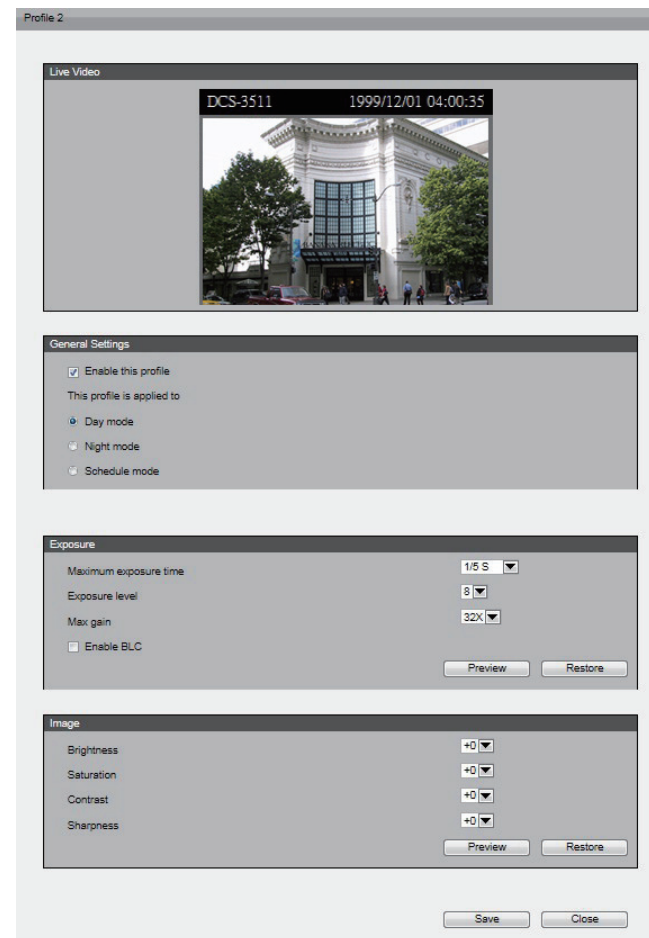
- The "Sensor Settings" and "Image Settings" share the same Profile 2 settings.

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.



Audio Settings

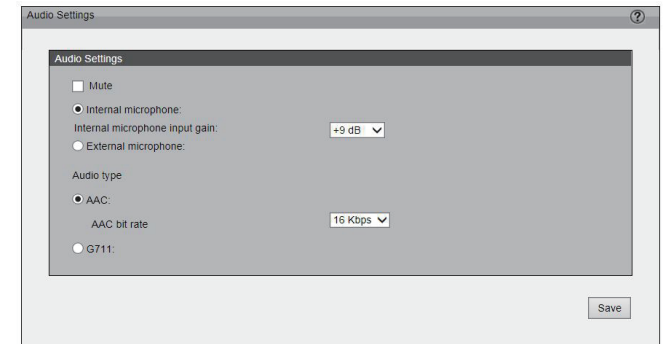
Mute: Select to mute audio.

Microphone input gain: It is necessary to find the optimum gain between -15dB to +15dB that transmits the best audio for listening.

Audio type: Advanced Audio Coding (AAC) is a wide band audio coding algorithm that exploits two primary coding strategies to dramatically reduce the amount of data needed to convey high-quality digital audio. Select a higher bit rate number for better audio quality.

AAC bit rate: Select an AAC bit rate from the drop-down list. Higher bit rate means higher audio quality but it takes more network bandwidth to transmit.

G711 bit rate: Select an G711 bit rate from the drop-down list. Higher bit rate means higher audio quality but it takes more network bandwidth to transmit.



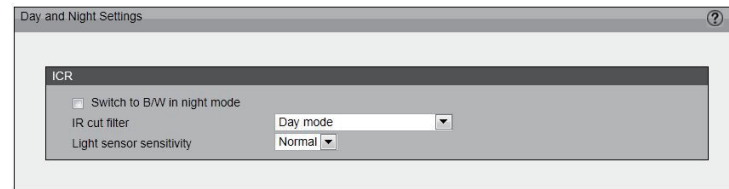
Day and Night Settings

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 06:00 and 18:00.

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



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 computer name and IP address.

The screenshot shows the 'IP Settings' window with the 'IPv4' section selected. Under 'LAN', the 'Get IP address automatically (DHCP)' option is selected. Other options include 'Use fixed IP address', 'Enable UPnP presentation', 'Enable UPnP port forwarding', and 'PPPoE'. A 'Save' button is visible at the bottom right.

The screenshot shows the 'IP Settings' window with the 'IPv4' section selected. Under 'LAN', the 'Use fixed IP address' option is selected. The configuration fields are filled with the following values: 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' options are unchecked. A 'Save' button is visible at the bottom right.

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

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 'IPv4' section selected. Under 'PPPoE', the 'User name' field is filled with '123456@hinet.net'. The 'Password' and 'Confirm password' fields are masked with dots. The 'LAN' and 'Use fixed IP address' options are not selected. A 'Save' button is visible at the bottom right.

The screenshot shows the 'IP Settings' window with the 'IPv4' section selected. Under 'LAN', the 'Get IP address automatically' option is chosen. The 'Enable UPnP presentation' checkbox is checked, while 'Enable UPnP port forwarding' is unchecked. The 'PPPoE' option is not selected. A 'Save' button is visible at the bottom right.

Wireless Settings

* Wireless function for DCS-3530 only

Enable Wireless: Click to enable wireless function.

Site Survey: Click the Rescan button to scan for available wireless networks. After scanning, you can use the drop-down box to select an available wireless network. The related information (SSID, Wireless Mode, Channel, Authentication, Encryption) will be automatically filled in for you.

SSID: Enter the SSID of the wireless access point you wish to use.

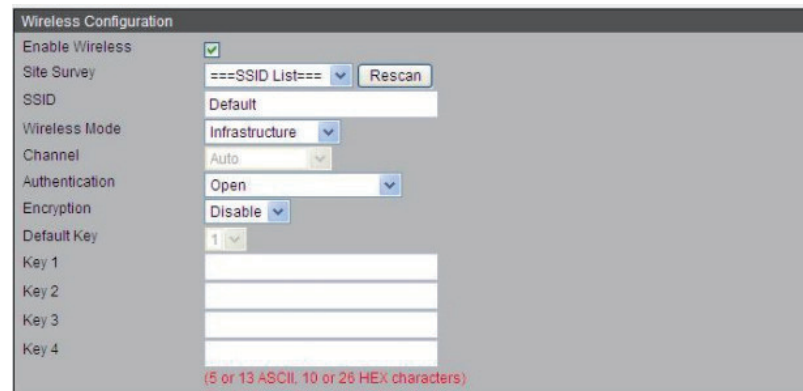
Wireless Mode: Use the drop-down box to select the mode of the wireless network you wish to connect to. Infrastructure is normally used to connect to an access point or router. Ad-Hoc is usually used to connect directly to another computer.

Channel: If you are using Ad Hoc mode, select the channel of the wireless network you wish to connect to, or select **Auto**.

Authentication: Select the authentication you use on your wireless network - Open, Shared, WPA-PSK, or WPA2-PSK.

Encryption: If you use WPA-PSK or WPA2-PSK authentication, you will need to specify whether your wireless network uses TKIP or AES encryption. If you use Open or shared authentication, WEP encryption should be the setting.

Default Key: If you use WEP, WPA-PSK, or WPA2-PSK authentication, enter the Key (also known as password) used for your wireless network.



The screenshot displays the 'Wireless Configuration' window. It includes the following settings:

- Enable Wireless:** A checked checkbox.
- Site Survey:** A dropdown menu showing '===SSID List===' and a 'Rescan' button.
- SSID:** A text field containing 'Default'.
- Wireless Mode:** A dropdown menu set to 'Infrastructure'.
- Channel:** A dropdown menu set to 'Auto'.
- Authentication:** A dropdown menu set to 'Open'.
- Encryption:** A dropdown menu set to 'Disable'.
- Default Key:** A dropdown menu set to '1'.
- Key 1, Key 2, Key 3, Key 4:** Four empty text input fields.

At the bottom right of the window, there is a red note: '(5 or 13 ASCII, 10 or 26 HEX characters)'.

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.

Note: JPEG only transmits a series of JPEG images to the client. In order to utilize this audio feature, make sure the video mode is set to H.264 or MPEG-4 and the media option in "Client Settings" is set to Video and Audio.

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 port/Secondary HTTP port

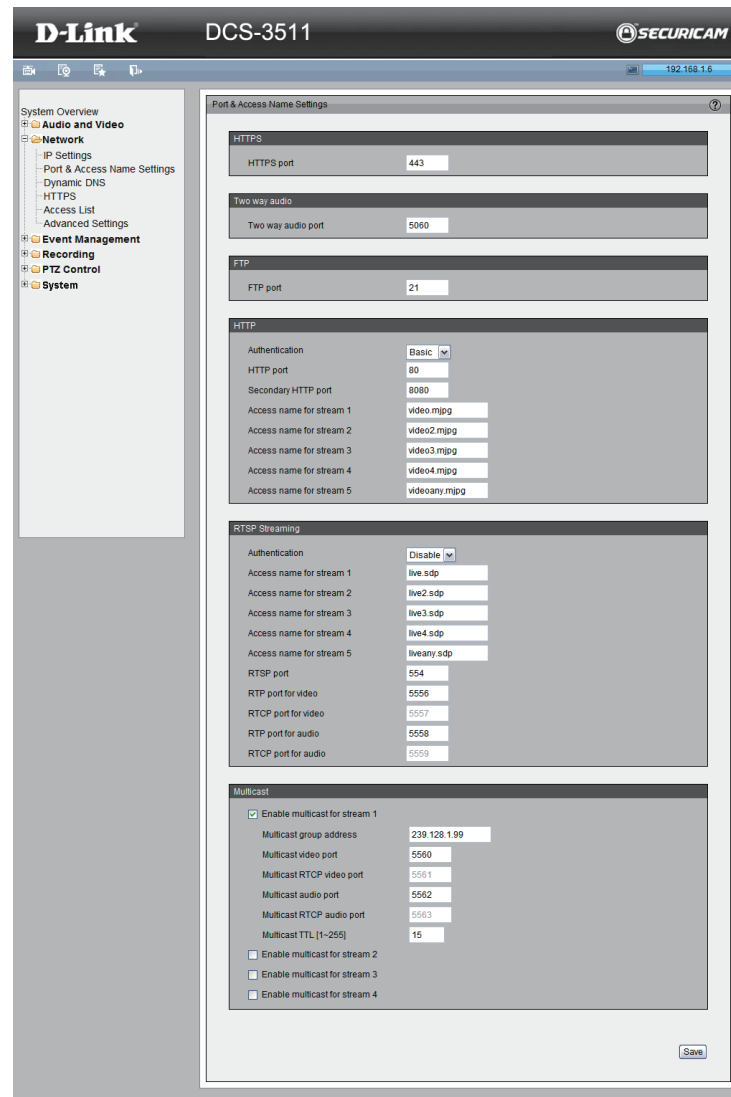
They can also be assigned to another port number between 1025 and 65535. To access the Network Camera on the LAN, both the HTTP port and secondary HTTP port can be used to access the Network Camera. For example, when the HTTP port is set to 80 and the secondary HTTP port is set to 8080. You can login camera as example link as below:

Http://192.168.0.20 or

Http://192.168.0.20:8080

Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via HTTP protocol: disable, basic, and digest. If basic authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If digest authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.

Access name for stream 1 ~ 4: This Network Camera supports multiple streams



simultaneously. The access name is used to differentiate the streaming source. When using Mozilla Firefox or Netscape to access the Network Camera and the video mode is set to JPEG, users will receive video comprised of continuous JPEG images. This technology, known as “server push”, allows the Network Camera to feed live pictures to Mozilla Firefox and Netscape. And use the following HTTP URL command to request transmission of the streaming data.

For example: `http://<ip address>:<http port>/<access name for stream 1 ~ 4>`

For example, when the Access name for stream 3 is set to video3.mjpg:

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

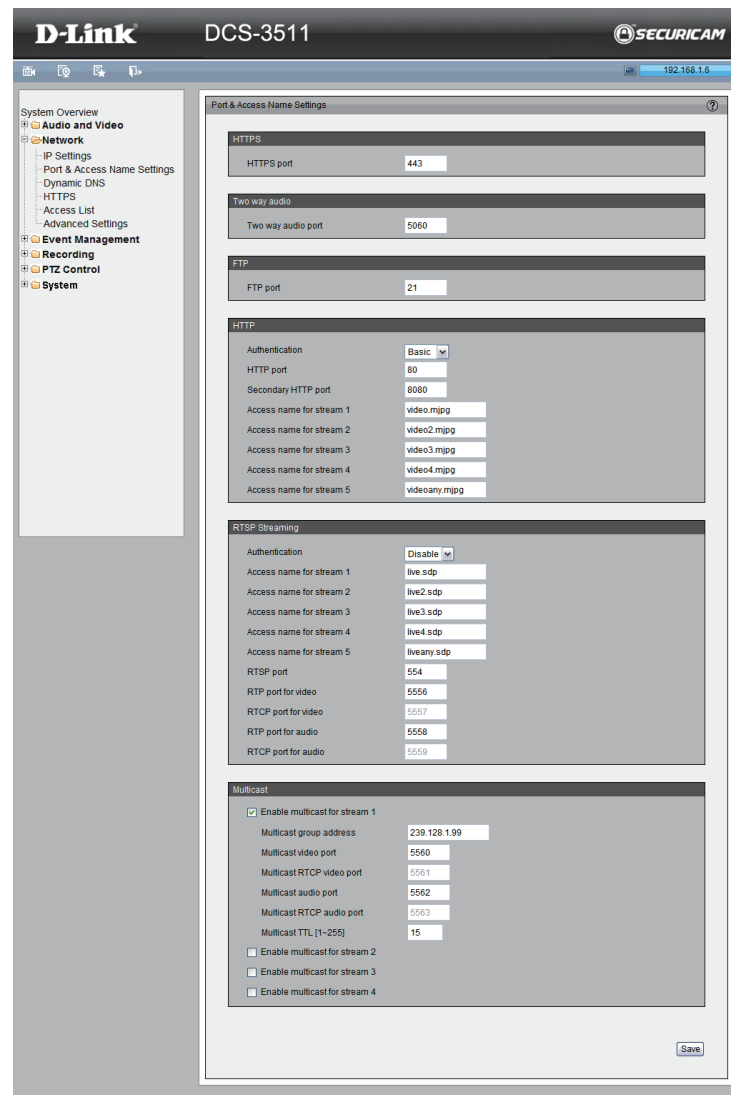
NOTE:

1. Microsoft® Internet Explorer does not support server push technology; therefore, using `http://<ip address>:<http port>/<access name for stream 1 ~ 4>` will fail to access the Network Camera.

RTSP

Authentication: Depending on your network security requirements, the Network Camera provides three types of security settings for streaming via RTSP protocol: disable, basic, and digest. If basic authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted. If digest authentication is selected, user credentials are encrypted using MD5 algorithm, thus providing better protection against unauthorized access.

Access name for stream 1 ~ 4: This Network Camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. If you want to use an RTSP player to access the Network Camera, you have to set the video mode to H.264 / MPEG-4 and use the following RTSP URL command to



request transmission of the streaming data.

RTSP port /

RTP port for video, audio/

RTCP port for video, audio

RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.

The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.

The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

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

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

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.

Multicast RTP video, audio port/

Multicast RTCP video, audio port

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

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

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.

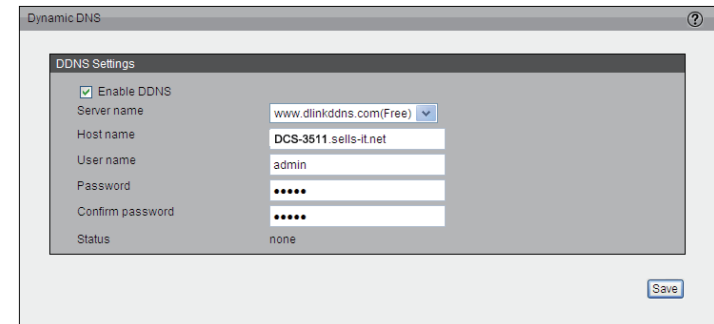
Server Name: Select a DDNS server name from the provider drop-down list. With a Dynamic DNS account, the camera automatically updates your IP address. To enable DDNS, enter your host information. Click **Next** to continue.

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-3511.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.

The screenshot shows the 'HTTPS' configuration window. It is divided into three main sections:

- Enable HTTPS:** This section has a checked checkbox for 'Enable HTTPS secure connection'. Below it are two radio button options: 'HTTP & HTTPS' (selected) and 'HTTPS only'.
- Create and install certificate method:** This section has three radio button options: 'Create self-signed certificate automatically', 'Create self-signed certificate manually' (selected), and 'Create certificate request and install'. Below the 'Create self-signed certificate manually' option is a 'Self-signed certificate:' label and a 'Create' button.
- Certificate Information:** This section displays the following 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

 At the bottom of this section are 'Property' and 'Remove' buttons.

Create Certificate Request and Install

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 a web interface for configuring HTTPS. It is titled "HTTPS" and contains three main sections:

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

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

At the bottom of this section are "Property" and "Remove" buttons.

Access List

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

General Settings

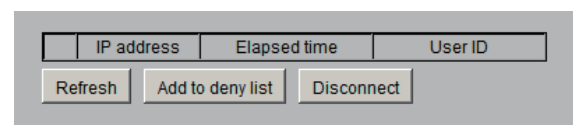
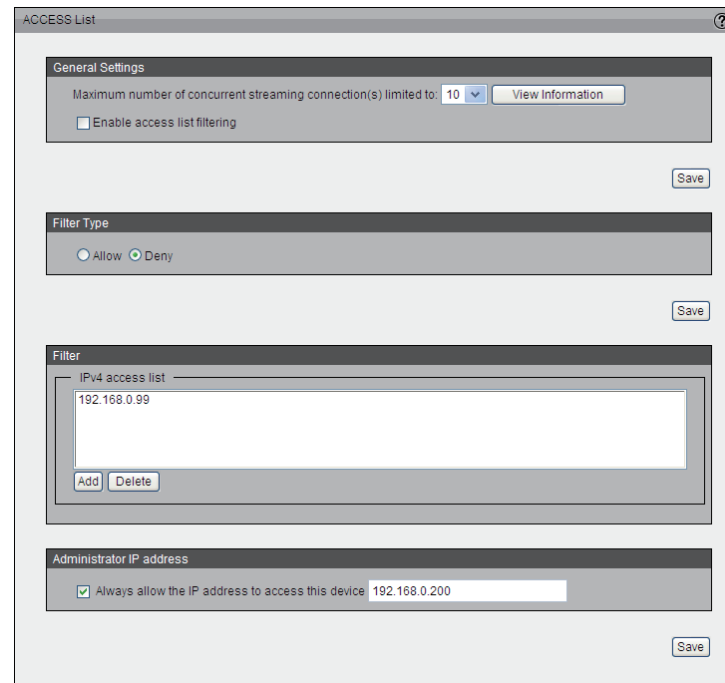
Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 ~ stream 5). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt to re-link (I.E. Explorer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

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 web interface. It is divided into four main sections:

- SNMP Configuration:** Contains two sub-sections. The first, 'Enable SNMPv1, SNMPv2c', has checkboxes for 'Read/Write community' (set to 'Private') and 'Read only community' (set to 'Public'). The second, 'Enable SNMPv3', has checkboxes for 'Read/Write Security name' (set to 'Private') and 'Read only Security name' (set to 'Public'). Both sections have dropdown menus for 'Authentication Type' (set to 'MD5') and input fields for 'Authentication Password' and 'Encryption Password'.
- IEEE 802.1x:** Features a checked 'Enable IEEE 802.1x' checkbox. The 'EAP method' is set to 'EAP-PEAP'. There are input 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' checkbox. It includes dropdown menus for 'VLAN ID' (set to '1'), 'Live Video' (set to '0'), 'Event/Alarm' (set to '0'), and 'Management' (set to '0').
- QoS/DSCP:** Has a checked 'Enable QoS/DSCP' checkbox. It includes dropdown menus for 'Live Video' (set to '0'), 'Event/Alarm' (set to '0'), and 'Management' (set to '0').

'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.

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

- SNMP Configuration:** This section is expanded and contains two sub-sections. The first sub-section has 'Enable SNMPv1, SNMPv2c' checked, with 'Read/Write community' set to 'Private' and 'Read only community' set to 'Public'. The second sub-section has 'Enable SNMPv3' checked, with 'Read/Write Security name' set to 'Private', 'Authentication Type' set to 'MD5', and 'Read only Security name' set to 'Public'. Both sub-sections have empty fields for 'Authentication Password' and 'Encryption Password'. A 'Save' button is located at the bottom right of this section.
- IEEE 802.1x:** This section has 'Enable IEEE 802.1x' checked. The 'EAP method' is set to 'EAP-PEAP'. There are empty fields for 'Identity' and 'Password'. The 'CA certificate' field is empty, with 'Browse...' and 'Upload' buttons next to it. The status is 'no file' and there is a 'Remove' button.
- CoS:** This section has 'Enable CoS' checked. The 'VLAN ID' is set to '1'. There are three dropdown menus for 'Live Video', 'Event/Alarm', and 'Management', all of which are currently set to '0'.
- QoS/DSCP:** This section has 'Enable QoS/DSCP' checked. There are three input fields for 'Live Video', 'Event/Alarm', and 'Management', all of which are currently set to '0'. A 'Save' button is located at the bottom right of this section.

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, 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.

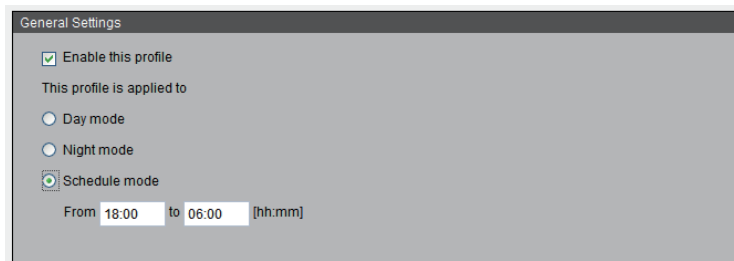
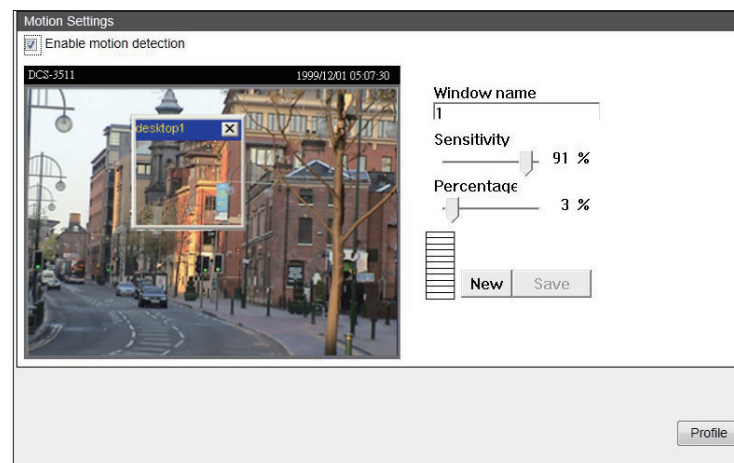
Note: Setting a higher sensitivity and a lower percentage will make motion easier to be detected.

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.



Profile:

You can configure two sets of sensor setting: one for normal situations(Profile1), the other for special situations(Profile2), such as day/night/schedule mode.

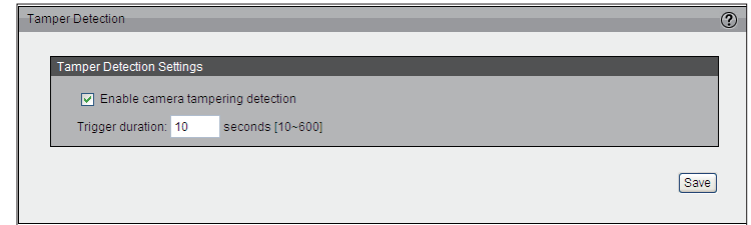
Tamper Detection

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:

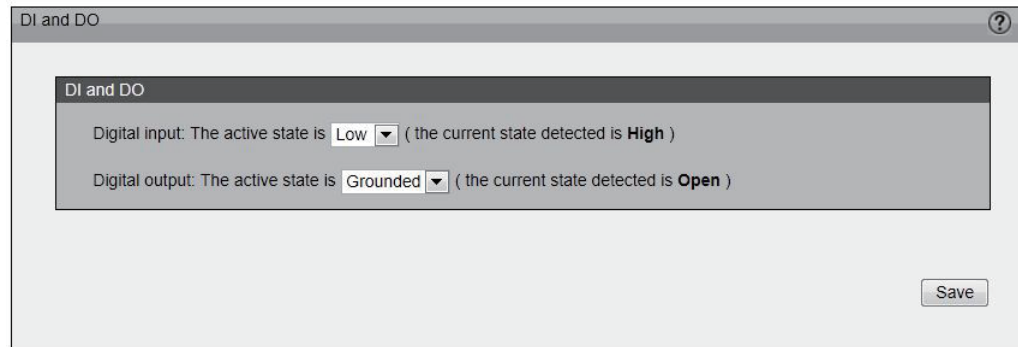
1. Select **Enable camera tampering detection**.
2. Enter the tamper trigger duration (10 sec. ~ 10 min.). The tamper alarm will be triggered only when the tampering factor (the difference between current frame and pre-saved background) exceeds the trigger threshold.

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.

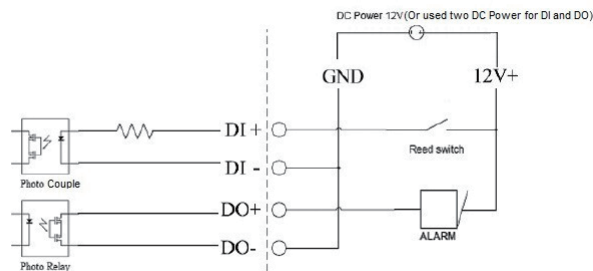


DI and DO

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+, GND) 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.

Sever 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.

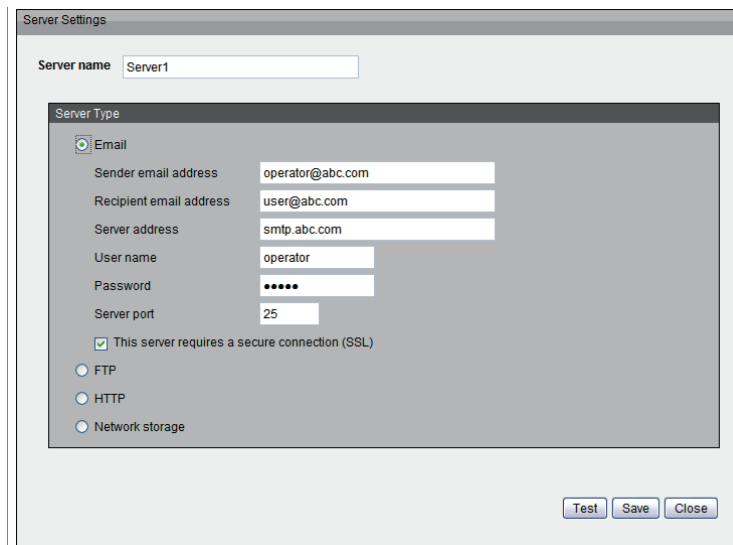
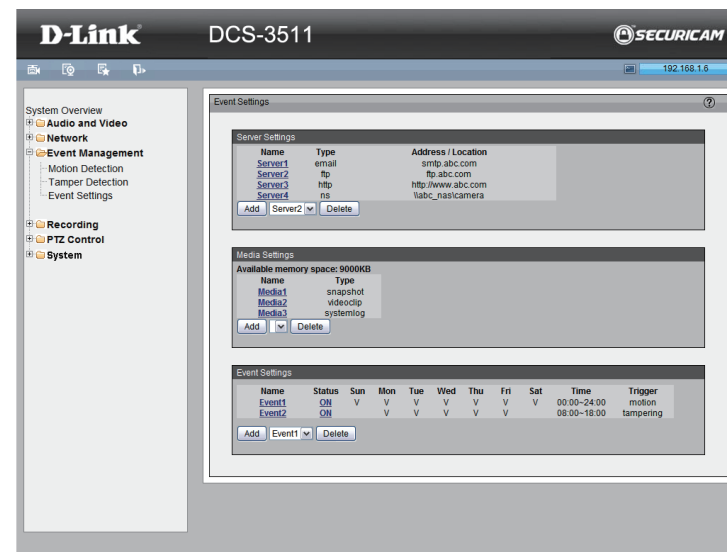
If your SMTP server requires a secure connection (SSL), select **This server requires a secure connection (SSL)**.

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.

The screenshot shows the 'Server name' field set to 'Server2'. The 'Server Type' section has 'FTP' selected. The 'Server address' is 'ftp.abc.com', 'Server port' is '21', 'User name' is 'operator', and 'Password' is masked with dots. The 'FTP folder name' field is empty. The 'Passive mode' checkbox is checked. At the bottom, there are 'Test', 'Save', and 'Close' buttons.

The screenshot shows the 'Server name' field set to 'Server3'. The 'Server Type' section has 'HTTP' selected. The 'URL' is 'http://www.abc.com', 'User name' is 'operator', and 'Password' is masked with dots. At the bottom, there are 'Test', 'Save', and 'Close' buttons.

The screenshot shows the 'Server name' field set to 'Server4'. The 'Server Type' section has 'Network storage' selected. The 'Network storage location' is '\\abc_nas\camera', with a note '(For example: \\my_nas\disk\folder)'. The 'Workgroup' is 'ipcam', 'User name' is 'operator', and 'Password' is masked with dots. At the bottom, there are 'Test', 'Save', and 'Close' buttons.

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.

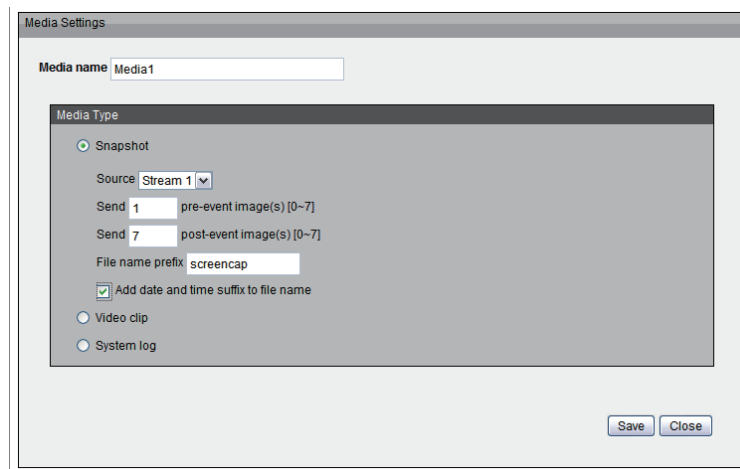
Add date and time suffix to the file name: Select this option to add a date/time suffix to the file name.

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.



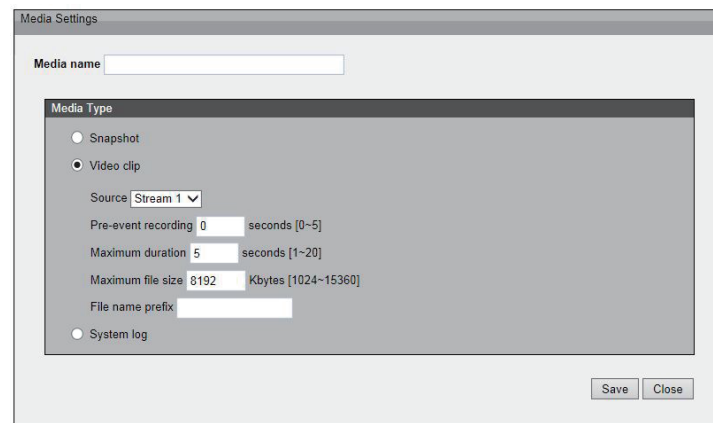
The screenshot shows a 'Media Settings' window with a 'Media name' field containing 'Media1'. Below it is a 'Media Type' section with three radio buttons: 'Snapshot' (selected), 'Video clip', and 'System log'. Under 'Snapshot', there is a 'Source' dropdown menu set to 'Stream 1', a 'Send' field with '1' for 'pre-event image(s) [0~7]', and another 'Send' field with '7' for 'post-event image(s) [0~7]'. There is also a 'File name prefix' field containing 'screencap' and a checked checkbox for 'Add date and time suffix to file name'. At the bottom right of the window are 'Save' and 'Close' buttons.

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 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.



Media Settings

Media name

Media Type

Snapshot

Video clip

Source

Pre-event recording seconds [0-5]

Maximum duration seconds [1-20]

Maximum file size Kbytes [1024-15360]

File name prefix

System log

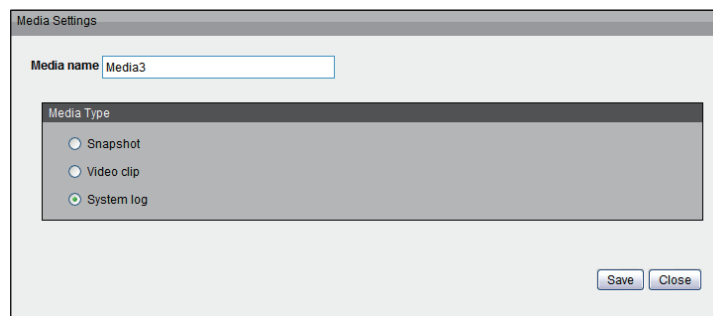
System log: Select to send a system log when a trigger is activated.

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.



Media Settings

Media name

Media Type

Snapshot

Video clip

System log

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. 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' configuration window. At the top, there is a text input field for 'Event name' containing 'Event1'. Below it is a checked checkbox for 'Enable this event'. A 'Priority' dropdown menu is set to 'Normal'. A text input field for 'Detect next event after' contains the number '3', followed by the text 'second(s)'. A note below states: 'Note: This can only be applied to motion detection and digital input'. The 'Trigger' section is highlighted with a dark header and contains several radio button options: 'Video motion detection' (selected), 'Normal', 'Profile', 'Periodically', 'System boot', 'Recording notify', and 'Camera Tampering Detection'. A note under 'Profile' says: 'Note: Please configure [Motion Detection](#) first'. The 'Event Schedule' section has a row of checkboxes for each day of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat), all of which are checked. Below this, there is a 'Time' section with 'Always' selected and a 'From' field set to '00:00' and a 'to' field set to '24:00' with the unit '[hh:mm]'. At the bottom right, there are 'Save' and 'Close' buttons.

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.

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 the 'Event Settings' window with the following configuration:

- Event name:** Event2
- Enable this event**
- Priority:** Normal
- Detect next event after:** 5 second(s)
- Note:** This can only be applied to motion detection and digital input
- Trigger:**
 - Video motion detection
 - Periodically
 - System boot
 - Recording notify
 - Camera Tampering Detection**Note:** Please configure [Camera Tampering Detection](#) first
- Event Schedule:**
 - Days: Sun Mon Tue Wed Thu Fri Sat
 - Time:**
 - Always
 - From 08:00 to 18:00 [hh:mm]

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).

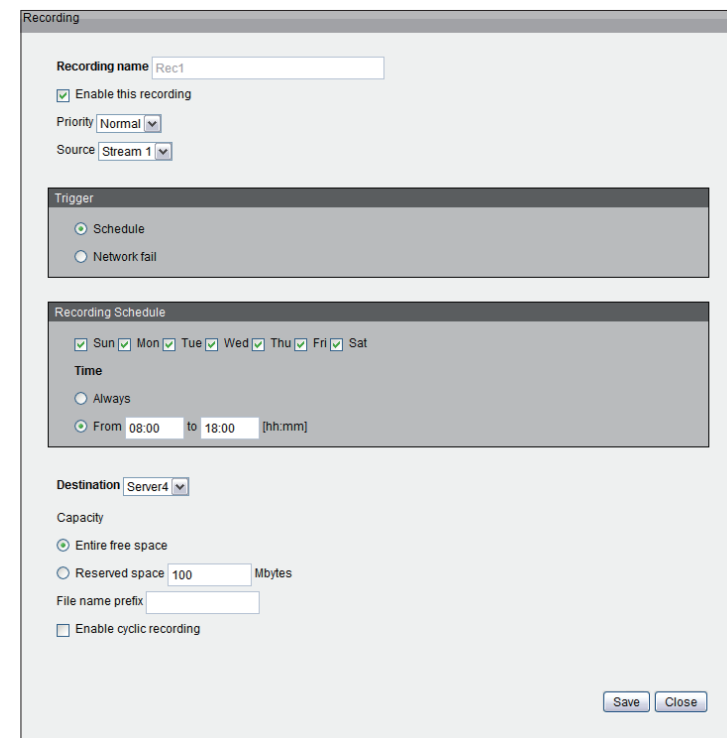
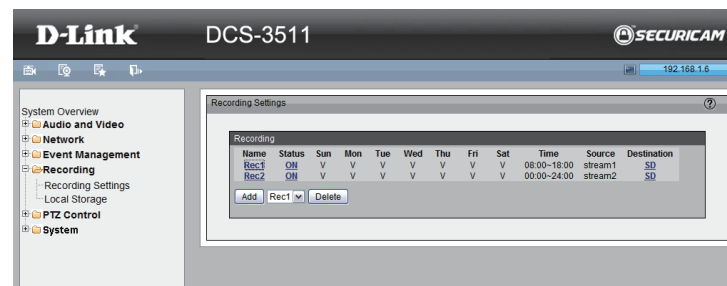
Recording Schedule: Specify the recording duration.

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 or local SD card 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.



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**.

Local Storage

This section explains how to manage the local storage on the Network Camera. Here you can view SD card status, search for recorded files to playback, download, etc.

SD Card Management

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

SD card control: Enable cyclic storage: Check this item if you want to enable cyclic recording. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.

Enable automatic disk cleanup: Check this item and enter the number of days you wish to retain a file. For example, if you enter “7 days”, the recorded files will be stored on the SD card for 7 days. Click Save to enable your settings.

Searching and Viewing the Records

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

File attributes: Select one or more items as your search criteria.

Trigger time: Manually enter the time range you want to search. Click Search and the recorded data corresponding to the search criteria will be listed in Search Results Window.

Search Results

This area will show the search results. There are four columns: Trigger time, Media type, Trigger type, and Locked. Click up and down arrow to sort the search results in either direction.

The screenshot shows the 'Local Storage' configuration page for a D-Link DCS-3511 camera. The interface includes a navigation menu on the left with categories like System Overview, Audio and Video, Network, Event Management, Recording, Recording Settings, Local Storage, PTZ Control, and System. The main content area is titled 'Local Storage' and contains the following sections:

- SD Card Management:** Displays SD card status (Ready), total size (2007176 KBytes), free size (1722396 KBytes), used size (284780 KBytes), and use percentage (14.19%). It includes a 'Format' button and 'SD card control' options: 'Enable cyclic storage' (checked), 'Enable automatic disk cleanup' (checked), and 'Maximum duration for keeping files: 7 days'. A 'Save' button is at the bottom.
- Searching and Viewing the Records:** Contains 'File attributes' with checkboxes for Trigger type (Tampering, System boot, Periodically, Digital input, Recording notify, Network fail, Video loss, Motion) and Media Type (Video clip, Snapshot, Text). It also has 'Locked' (Locked/Unlocked) and 'Trigger time' (From/To date and time) fields. A 'Search' button is at the bottom.
- Search Results:** Shows a table of search results with columns for Trigger time, Media type, Trigger type, and Locked. The table contains 12 entries, with the first two checked. Below the table are buttons for 'View', 'Download', 'Uncheck All', 'JPEGs to AVI', 'Lock / Unlock', and 'Remove'. A note states: 'Note: "View" and "Download" only apply to the highlight item'.

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:

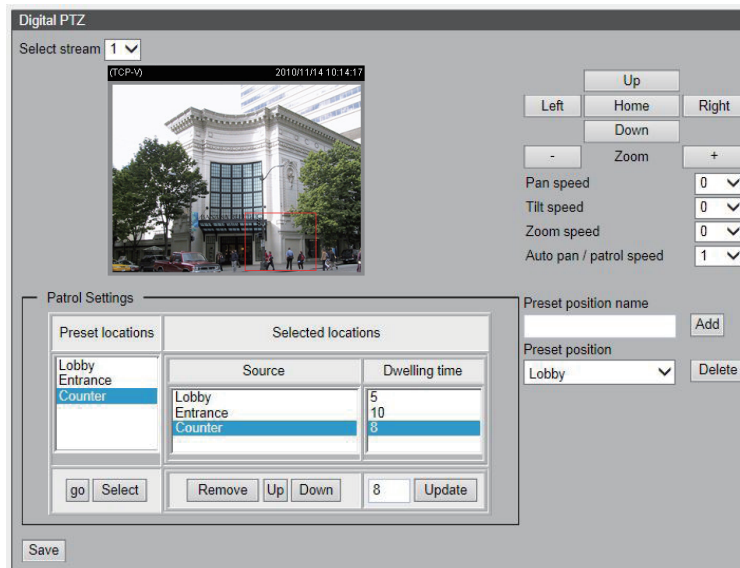
1. Adjust the shooting area to the desired position using the buttons on the right side of the window.
2. Enter a name for the preset position, which allows for up to forty characters. Click **Add** to enable the Setting. The preset positions will be displayed under the Preset Location list on the left-hand 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.



Mechanical PTZ

To utilize this feature, please connect the camera to a PTZ driver or scanner via RS485 interface first. Then you can configure the PTZ driver and RS485 port with the following setting.

Enable Mechanical PTZ Operation: Select this option to enable this function.

Camera ID: The Camera ID is necessary to control multiple cameras. If you click **Save** to enable this function, the camera control panel will be displayed on the main page.

Camera ID: This ID is the identifier for RS-485 devices. IDs range from 1 to 255.

PTZ Driver: The camera supports Pelco D & P protocol PTZ driver. If your PTZ scanner does not support above driver, please select Custom camera (scanner). Please refer to the user's manual of your PTZ scanner to determine the Camera ID, PTZ driver, and Port setting.

Baud Rate: Baud Rate is a speed measurement for communication between a transmitter and receiver which indicates the number of bit transfers per second. A higher baud rate will reduce the distance of the two devices (transmitter and receiver). Values range from 2400 (default) to 19200 bps.

Data Bits: This value is the number of data bits in a transmission. The data bit can be 7 or 8 (default).

Stop Bits: The stop bit is used to signal the end of communication for a single packet. The more bits used for stop bits, the greater the lenience in synchronizing the different clocks but the slower the data transmission rate. The stop bit can be set to 1 or 2. The default value is 1.

Parity Bit: Parity is a form of error checking used in serial communication. For even and odd parities, the serial port sets the parity bit (the last bit after the data bits) to a value to ensure that the transmission has an even or odd number of logic high bits. For example, if the data is 011, for even parity, the parity bit is 0 to keep the number of logic-high bits even. If the parity is odd, the parity bit is 1, resulting in 3 logic-high bits. Parity can be set to No (none), Even, and Odd.

Preset Position: Clicking this button returns the camera to a preset position.

Custom Command: Clicking this button allows you to define up to five custom commands for your PTZ scanner.

Mechanical PTZ

Enable Mechanical PTZ Operation

Camera ID: 1

PTZ driver: None

Baud rate: 9600

Data bits: 8

Stop bits: 1

Parity bit: None

Preset position Custom Command

Save

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.

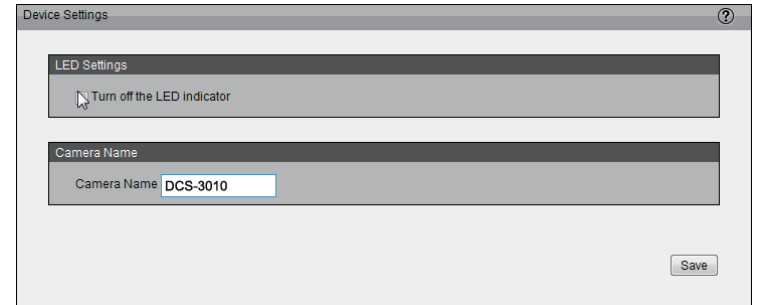
The screenshot displays the 'User Settings' web interface, which is organized into three main sections:

- 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 showing '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.



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.

Daylight saving time: At some area, the clocks are adjusted one hour forward during the warmer months in a year. Set the start and end date and time of Daylight saving time according to your location.

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 the 'Time and Date' configuration window. It is divided into three main sections:

- Time Configuration:** Displays the current server time as '3 Nov 2014 17:18:59'. The time zone is set to 'GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei'. There is a checkbox for 'Enable daylight saving' which is currently unchecked. Below this, the 'Daylight saving time' section includes dropdown menus for 'DST start' (Month: Mar, Week: 1st, Day of week: Sun, Time: 12 am) and 'DST end' (Month: Nov, Week: 1st, Day of week: Sun, Time: 12 am).
- Automatic Time Configuration:** Features a checkbox for 'Enable Automatic Time Configuration' which is unchecked. It includes an 'NTP server' dropdown menu with a '<< Select NTP server' button and an 'Updating interval' dropdown menu set to 'One day'.
- Set the Date and Time Manually:** Contains dropdown menus for 'Year' (2014), 'Month' (11), 'Day' (03), 'Hour' (17), 'Minute' (18), and 'Second' (59). A 'Copy Your Computer's Time Settings' button is located below these fields.

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.

Schedule Reboot: Select this option to schedule a time for the device to reboot.

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.

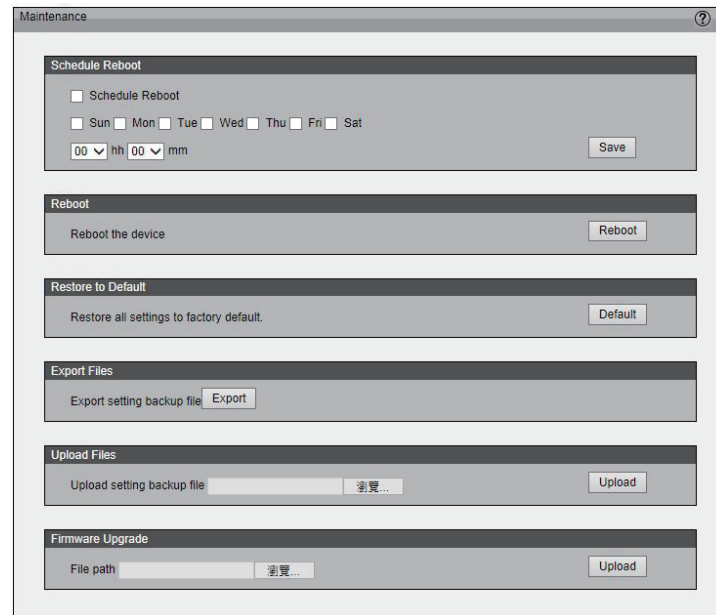
Export / Upload Files: This feature allows you to Export / Upload setting backup files.

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!



The screenshot shows a web interface titled "Maintenance" with a help icon in the top right corner. The interface is divided into several sections:

- Schedule Reboot:** Contains a checkbox for "Schedule Reboot". Below it are checkboxes for days of the week: Sun, Mon, Tue, Wed, Thu, Fri, Sat. There are also dropdown menus for "hh" (set to 00) and "mm" (set to 00), and a "Save" button.
- Reboot:** Contains a "Reboot the device" button and a "Reboot" button.
- Restore to Default:** Contains a "Restore all settings to factory default." button and a "Default" button.
- Export Files:** Contains an "Export setting backup file" button and an "Export" button.
- Upload Files:** Contains an "Upload setting backup file" text input, a "浏览..." (Browse...) button, and an "Upload" button.
- Firmware Upgrade:** Contains a "File path" text input, a "浏览..." (Browse...) button, and an "Upload" button.

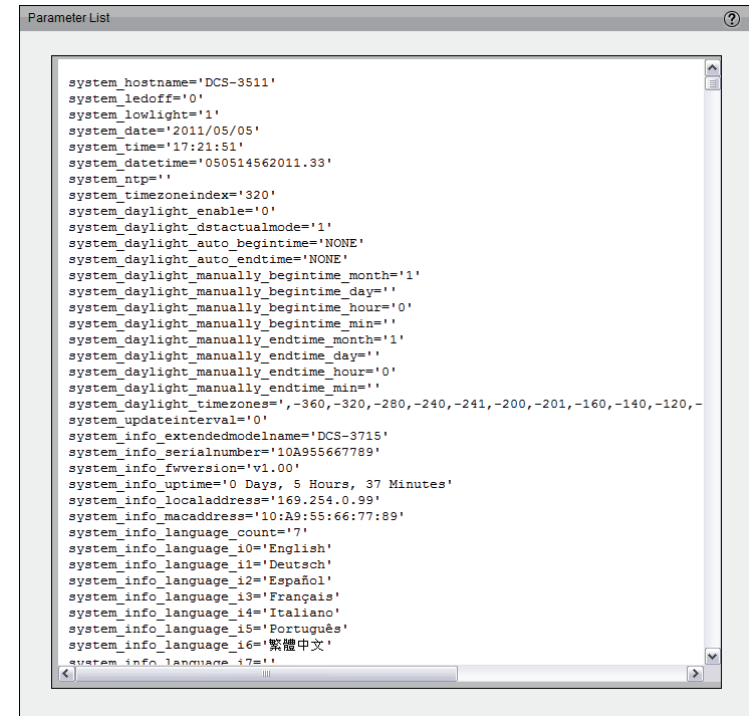
Follow the steps below to upgrade the firmware:

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.

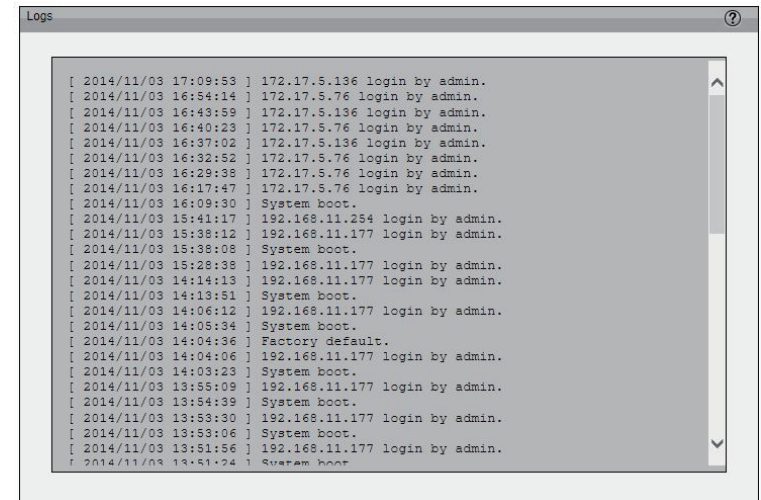


```
system_hostname='DCS-3511'  
system_ledoff='0'  
system_lowlight='1'  
system_date='2011/05/05'  
system_time='17:21:51'  
system_datetime='050514562011.33'  
system_ntp=''  
system_timezoneindex='320'  
system_daylight_enable='0'  
system_daylight_detactualmode='1'  
system_daylight_auto_begintime='NONE'  
system_daylight_auto_endtime='NONE'  
system_daylight_manually_begintime_month='1'  
system_daylight_manually_begintime_day='0'  
system_daylight_manually_begintime_hour='0'  
system_daylight_manually_begintime_min=''  
system_daylight_manually_endtime_month='1'  
system_daylight_manually_endtime_day='0'  
system_daylight_manually_endtime_hour='0'  
system_daylight_manually_endtime_min=''  
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-160,-140,-120,-  
system_updateinterval='0'  
system_info_extendedmodelname='DCS-3715'  
system_info_serialnumber='10A955667789'  
system_info_fwversion='v1.00'  
system_info_uptime='0 Days, 5 Hours, 37 Minutes'  
system_info_localaddress='169.254.0.99'  
system_info_macaddress='10:A9:55:66:77:89'  
system_info_language_count='7'  
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='Português'  
system_info_language_16='繁體中文'  
system_info_language_17=''
```


Logs

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

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.



The screenshot shows a window titled "Logs" with a scrollable list of system log entries. The entries are as follows:

```
[ 2014/11/03 17:09:53 ] 172.17.5.136 login by admin.
[ 2014/11/03 16:54:14 ] 172.17.5.76 login by admin.
[ 2014/11/03 16:43:59 ] 172.17.5.136 login by admin.
[ 2014/11/03 16:40:23 ] 172.17.5.76 login by admin.
[ 2014/11/03 16:37:02 ] 172.17.5.136 login by admin.
[ 2014/11/03 16:32:52 ] 172.17.5.76 login by admin.
[ 2014/11/03 16:29:38 ] 172.17.5.76 login by admin.
[ 2014/11/03 16:17:47 ] 172.17.5.76 login by admin.
[ 2014/11/03 16:09:30 ] System boot.
[ 2014/11/03 15:41:17 ] 192.168.11.254 login by admin.
[ 2014/11/03 15:38:12 ] 192.168.11.177 login by admin.
[ 2014/11/03 15:38:08 ] System boot.
[ 2014/11/03 15:28:38 ] 192.168.11.177 login by admin.
[ 2014/11/03 14:14:13 ] 192.168.11.177 login by admin.
[ 2014/11/03 14:13:51 ] System boot.
[ 2014/11/03 14:06:12 ] 192.168.11.177 login by admin.
[ 2014/11/03 14:05:34 ] System boot.
[ 2014/11/03 14:04:36 ] Factory default.
[ 2014/11/03 14:04:06 ] 192.168.11.177 login by admin.
[ 2014/11/03 14:03:23 ] System boot.
[ 2014/11/03 13:55:09 ] 192.168.11.177 login by admin.
[ 2014/11/03 13:54:39 ] System boot.
[ 2014/11/03 13:53:30 ] 192.168.11.177 login by admin.
[ 2014/11/03 13:53:06 ] System boot.
[ 2014/11/03 13:51:56 ] 192.168.11.177 login by admin.
[ 2014/11/03 13:51:24 ] System boot.
```

Technical Specifications

DCS-3511/DCS-3530			
Camera	Hardware Profile	<ul style="list-style-type: none"> ▪ 1/4" 1 Megapixel CMOS sensor ▪ 2.8~12mm fixed lens ▪ Shutter speed 1/5 to 1/10,000 	<ul style="list-style-type: none"> ▪ Aperture F1.4 ▪ Angle of view <ul style="list-style-type: none"> ▪ 77.5~22.7° (H) ▪ 53.5~14.5° (V) ▪ 82.5~27° (D) ▪ Mini Object Distance (MOD):0.2M
	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 	<ul style="list-style-type: none"> ▪ 5 configurable privacy mask zones ▪ Configurable brightness, saturation, contrast, and sharpness ▪ Min Illumination: 0.1 Lux (color), 0.05Lux (BW)
	Video Compression	<ul style="list-style-type: none"> ▪ Simultaneous H.264/MPEG-4/MJPEG format compression ▪ H.264/MPEG-4 multicast streaming 	<ul style="list-style-type: none"> ▪ JPEG for still images
	Video Resolution	<ul style="list-style-type: none"> ▪ 16:9 - 1280 x 800, 1280 x 720, 640 x 360, 480 x 270, 320 x 176 up to 30 fps recording¹ 	<ul style="list-style-type: none"> ▪ 4:3 - 1024 x 768, 800 x 600, 640 x 480, 320 x 240 up to 30 fps recording¹
	Audio Features	<ul style="list-style-type: none"> ▪ G.711 audio encoding, bit rate: 8 kbps to 64 kbps ▪ MPEG-4 AAC audio encoding, bit rate: 16 kbps to 32 kbps 	
	External Device Interfaces	<ul style="list-style-type: none"> ▪ 10/100 BASE-TX Fast Ethernet port ▪ 802.11 b/g/n wireless (for DCS-3530 only) 	<ul style="list-style-type: none"> ▪ microSD card slot ▪ Dlx1, DOx1 ▪ RS485
Network	Network Protocols	<ul style="list-style-type: none"> ▪ IPv4 ▪ IPv6 ▪ TCP/IP ▪ UDP ▪ ICMP ▪ DHCP client ▪ NTP client (D-Link) ▪ DNS client ▪ DDNS client (D-Link) ▪ SMTP client ▪ SNMP ▪ FTP client ▪ HTTP / HTTPS 	<ul style="list-style-type: none"> ▪ Samba client ▪ PPPoE ▪ UPnP port forwarding ▪ RTP / RTSP/ RTCP ▪ IP filtering ▪ QoS ▪ CoS ▪ Multicast ▪ IGMP ▪ ONVIF compliant
	Security	<ul style="list-style-type: none"> ▪ Administrator and user group protection ▪ Password authentication ▪ HTTPS encryption for web browser 	<ul style="list-style-type: none"> ▪ HTTP and RTSP digest encryption ▪ Remote client access control

Appendix A - Technical Specifications

System Management	System Requirements for Web Interface	<ul style="list-style-type: none"> ▪ Browser: Internet Explorer, Firefox, Chrome
	Event Management	<ul style="list-style-type: none"> ▪ Motion detection ▪ Event notification and uploading of snapshots/video clips via e-mail or FTP ▪ Supports multiple SMTP and FTP servers ▪ Multiple event notifications ▪ Multiple recording methods for easy backup
	Remote Management	<ul style="list-style-type: none"> ▪ Take snapshots/video clips and save to local hard drive ▪ Configuration interface accessible via web browser
	Mobile Support	<ul style="list-style-type: none"> ▪ mydlink mobile app for iOS and Android mobile devices
	D-ViewCam™ System Requirements	<ul style="list-style-type: none"> ▪ Operating System: Microsoft Windows 7/Vista/XP ▪ Web Browser: Internet Explorer 7 or higher ▪ Protocol: Standard TCP/IP
	D-ViewCam™ Software Functions	<ul style="list-style-type: none"> ▪ Remote management/control of up to 32 cameras ▪ Viewing of up to 32 cameras on one screen ▪ Scheduled motion triggered, or manual recording options ▪ Supports all management functions in web interface
Physical	Weight	200 g (0.44lb)
	Power	12V DC 1.5 A, 802.3af PoE (for DCS-3511 only)
	Power Consumption	2.4W (12V DC), 2.88W (PoE).
	Temperature	<ul style="list-style-type: none"> ▪ Operating: 0 to 40 °C (32 to 104 °F) ▪ Storage: -20 to 70 °C (-4 to 158 °F)
	Humidity	<ul style="list-style-type: none"> ▪ Operating: 20% to 80% non-condensing ▪ Storage: 5% to 95% non-condensing
	Certifications	<ul style="list-style-type: none"> ▪ CE ▪ CE LVD ▪ FCC ▪ C-Tick
Dimensions	<p>The technical drawings show the following dimensions:</p> <ul style="list-style-type: none"> Front View: A hexagonal shape with a diameter of 68.9mm. Side View (Left): A length of 131.70mm and a height of 45.7mm. Side View (Right): A length of 149mm and a height of 112mm. 	

Order Information	
Part Number	Description
DCS-3511	HD PoE Network Camera
DCS-3530	HD Wireless N Network Camera