Version 1.0 | 10/15/2013

# User Manual

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

DCS-3511/DCS-3530

# 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 | October 15, 2013 | DCS-3511/DCS-3530 Revision A1 with firmware version 1.00 |

# Trademarks

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

Copyright ©2013 by D-Link 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**
Package Contents................................................................5
Minimum Requirements................................................................6
Introduction................................................................7
Features................................................................8
Hardware Overview................................................................9
Front Panel................................................................9
Rear Panel................................................................10
Side Panel................................................................11
Button Panel................................................................12

**Installation................................................................13**
Hardware Installation................................................................13
Configuration with Wizard................................................................14
Viewing Camera via Web Browser................................................................19
D-ViewCam Setup Wizard................................................................21

**Configuration................................................................23**
Live Video................................................................23
Client Setup................................................................27
Setup................................................................28
Standard Setup................................................................28
Advanced Setup................................................................29
System Overview................................................................30
Video................................................................31
Video Settings................................................................31
Image Settings................................................................34
Audio Settings................................................................36
Day and Night Settings................................................................37
Network................................................................38
IP Settings................................................................38
Wireless Settings................................................................40
Port and Access Name Settings................................................................41
Dynamic DNS................................................................44
HTTPS................................................................45
Access List................................................................47
Advanced Settings................................................................49
Event Management................................................................53
Motion Detection................................................................53
Tamper Detection................................................................54
DI and DO................................................................55
Event Settings................................................................56
Recording................................................................62
Recording Settings................................................................62
Local Storage................................................................64
PTZ Control................................................................65
Digital PTZ................................................................65
Mechanical PTZ................................................................66

System ....................................................................................67

User Settings ....................................................................67

Device Settings.................................................................68

Time and Date..................................................................69

Maintenance......................................................................70

Parameter List ..................................................................72

Logs ......................................................................................73

**Appendix A - Technical Specifications ............................ 74**

**Appendix B - Contacting Technical Support.................. 77**

**Appendix C - Warranty ..................................................... 78**

**Appendix D - Registration .............................................. 84**

# Package Contents

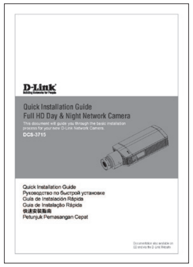
DCS-3511 or DCS-3530
HD Network Camera

Mounting Bracket

FULL HD DAY & NIGHT
Network Camera
Ver. 1.00(WW)
Contents
Installation Wizard
Installation Guide
Manual
D-Link
Building Networks for People
Business Class Networking
DCS-3715
©2010 D-Link Corporation/D-Link Systems, Inc. All Rights Reserved.

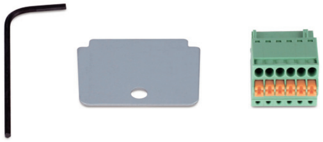
User Manual and Software on CD-ROM

Power Adapter


D-Link
Building Networks for People
Quick Installation Guide
Full HD Day & Night Network Camera
This document will guide you through the basic installation process for your new D-Link Network Camera.
DCS-3715
Quick Installation Guide
Руководство по быстрой установке
Guía de Instalación Rápida
Guia de Instalação Rápida
快速安裝指南
Petunjuk Pemasangan Cepat
Documentation also available on CD and via the D-Link Website

Quick Install Guide

CAT5 Ethernet Cable



Allen Wrench, lens ring fixture, and I/O connectors

Antenna
(DCS-3530 only)

Mic/Speaker Combo Cable

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

# Minimum Requirements

- Operating System: Windows® 8, 7, Vista®, or XP (Service Pack 2 or higher)
- Web Browser: Internet Explorer 7 or higher, Firefox, Chrome,  or Safari 4 or higher
- VGA card resolution: SVGA or XGA (1024x768 or above)
- CPU: 1.7GHz or above (2.8GHz plus processor with 512MB memory and a 32MB video card is required for multiple camera viewing and recording in IP surveillance program)
- An available Ethernet connection or Wireless network (DCS-3530 only)

# Introduction

DCS-3511/3530 are HD, full frame rate network cameras with H.264 compression. The DCS-3511/3530 connect to your network to provide high-quality live video over the Internet. With vivid video quality and superb high resolution, it can provide excellent detail of the video which is useful to identify any suspicious activity. The Network Camera provides multiple streaming and flexible viewing settings for different purposes of surveillance, either for regular recording or mobile view. You can record important events to a microSD card as a local backup.

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**

The Network Camera provides HD industrial standard 16:9 wide screen video for IP surveillance. With the varifocal lens, it is a high performance high quality network camera. The "viewing window" design can provide 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, pan, and tilt control.

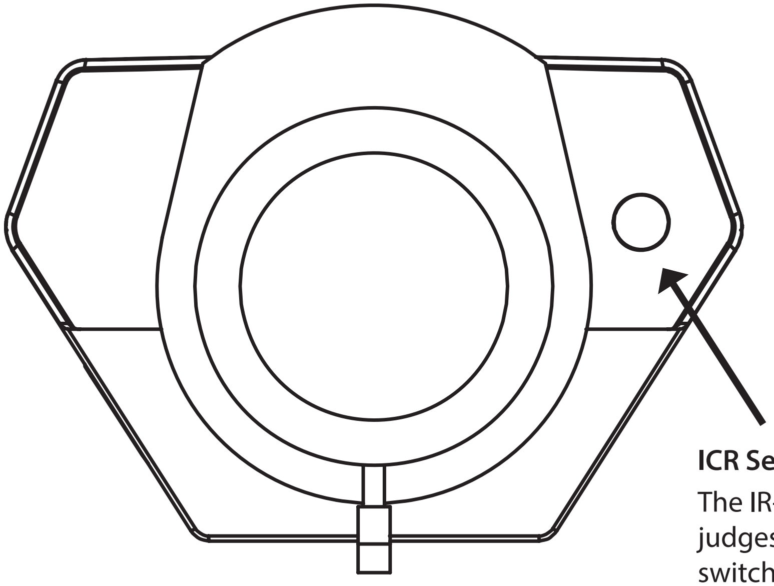
**Flexible Connectivity**

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

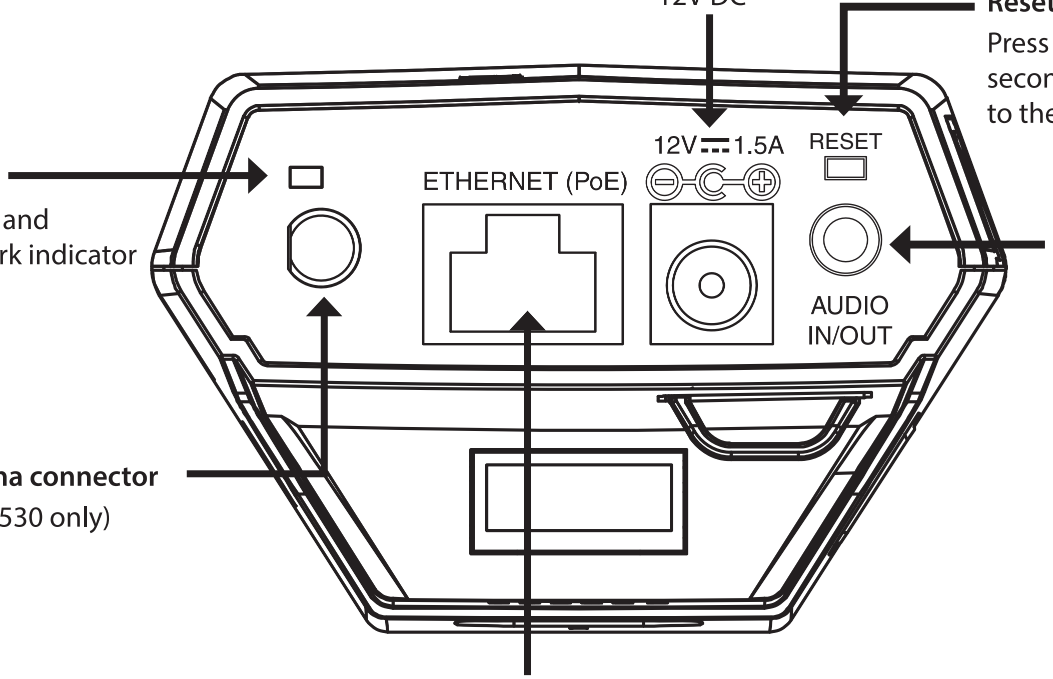
## Front Panel



**ICR Sensor**

The IR-Cut Removable sensor judges lighting conditions and switches from color to infrared accordingly

# Rear Panel



**DC Power**

12V DC

**Reset**

Press and hold this button for 10 seconds to reset the camera back to the factory default settings.

**LED**

Power and network indicator

**Audio Input/Output**

Use to connect an external microphone and/or speaker

**Antenna connector**

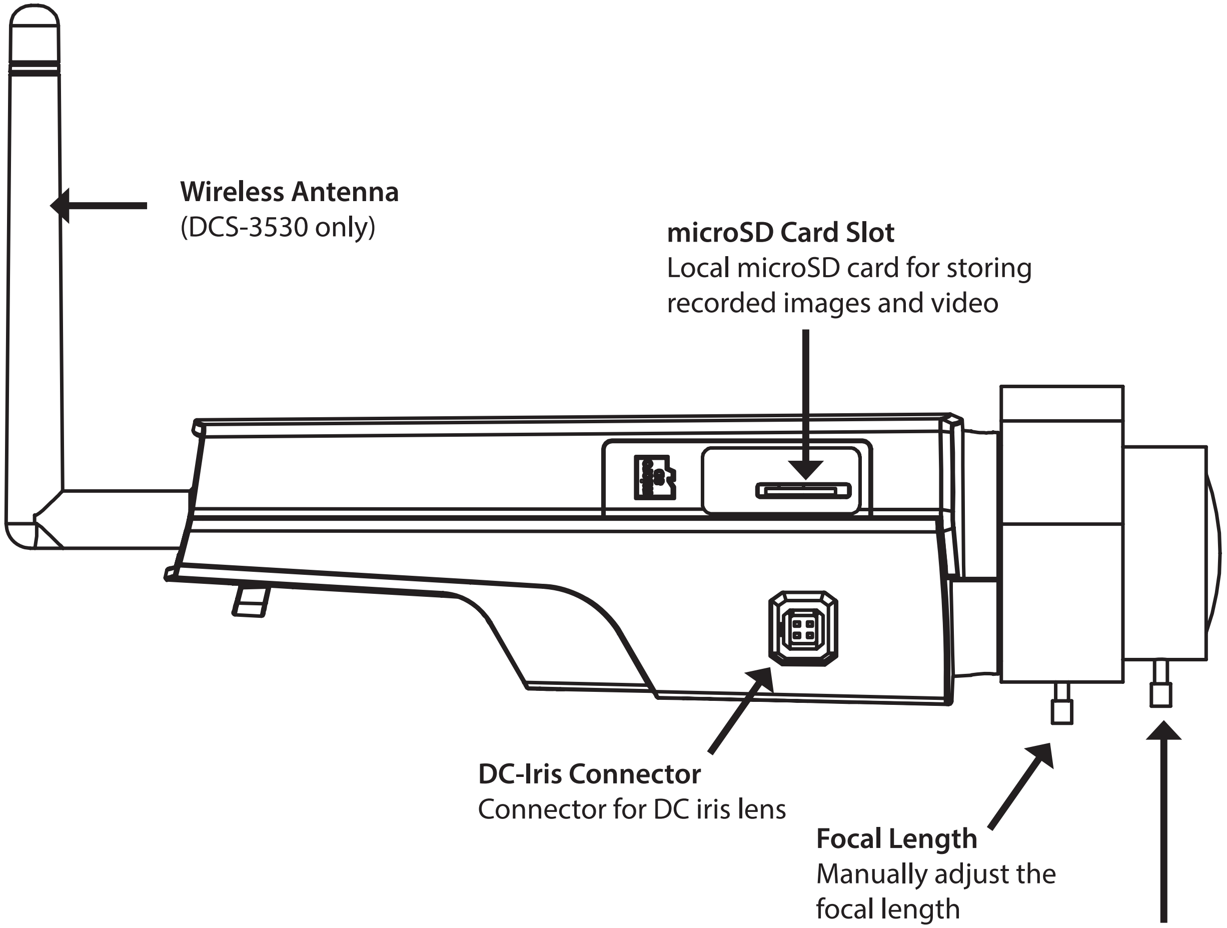
(DCS-3530 only)

**Ethernet (PoE)**

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

(PoE only available on the DCS-3511)

# Side Panel



**Wireless Antenna**
(DCS-3530 only)

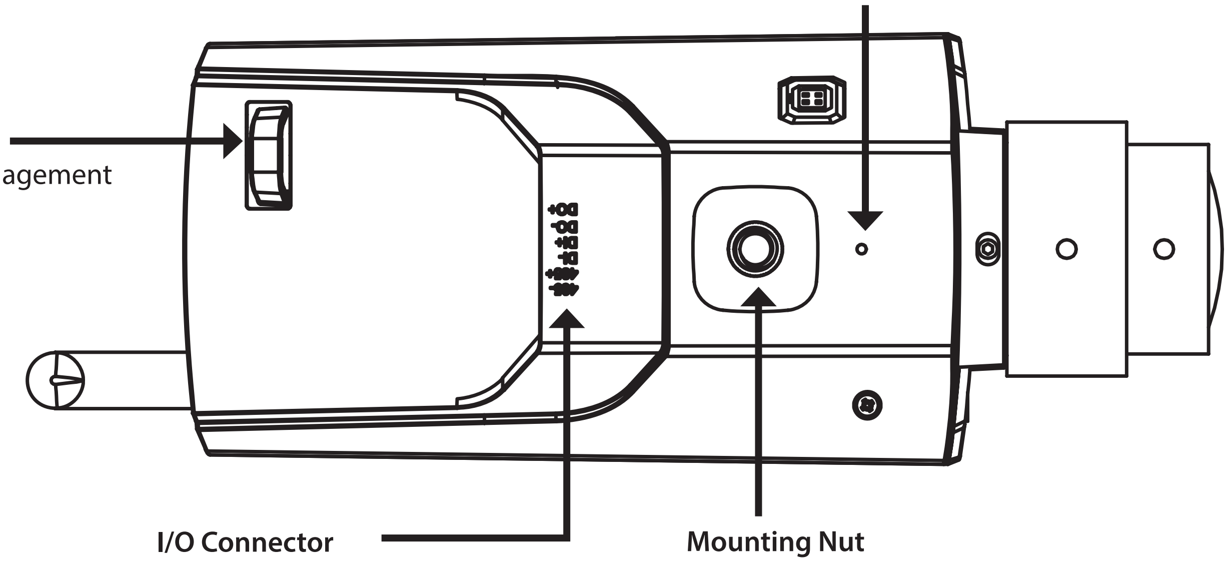
**microSD Card Slot**
Local microSD card for storing recorded images and video

**DC-Iris Connector**
Connector for DC iris lens

**Focal Length**
Manually adjust the focal length

**Focus**
Manually adjust focus

# Button Panel



**Built-in MIC**
Internal microphone

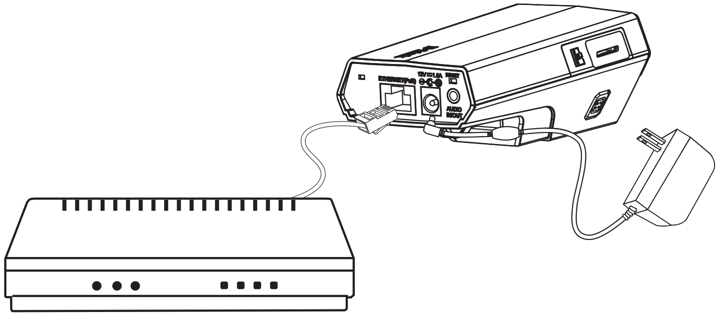
**Wire Clip**
Cable management

**I/O Connector**
I/O connectors for external devices

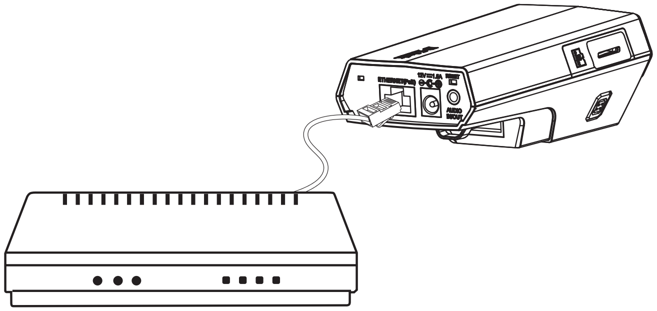
**Mounting Nut**
1/4' x 20 nut for affixing camera to mounting bracket

# 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.

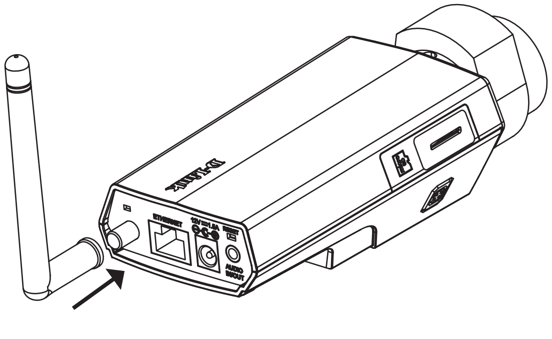


**Connection Using a PoE Switch**
If using a PoE switch, connect the network camera via Ethernet cable.
PoE will transmit both power and data over a single cable.



***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.*

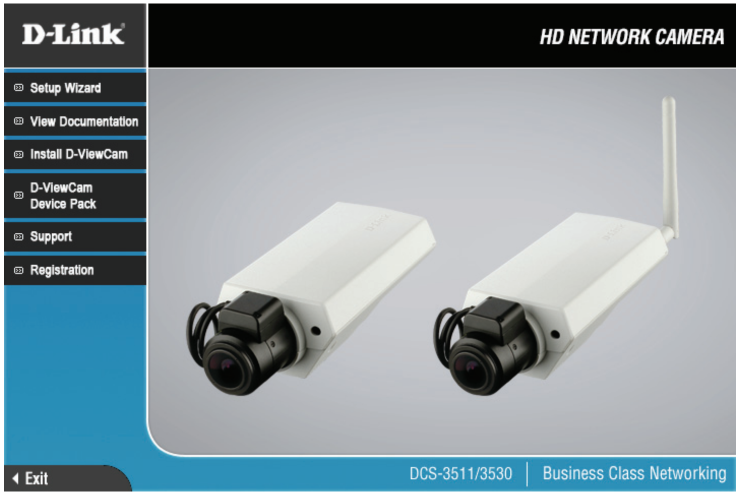
**Attach the Antenna (DCS-3530 only)**
Locate the antenna included with your DCS-3530 and attach it to the antenna connector located on the back of the DCS-3530.



# Configuration with Wizard

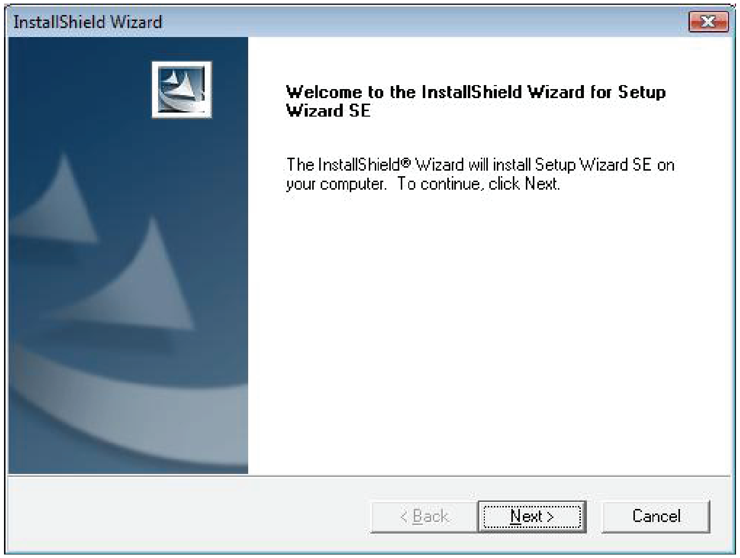
Insert the DCS-3511/DCS-3530 CD into your computer's CD-ROM drive to begin the installation. If the Autorun function on your computer is disabled, or if the D-Link Launcher fails to start automatically, click **Start > Run**. Type **D:\autorun.exe**, where D: represents the drive letter of your CD-ROM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

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



After clicking Setup Wizard, the following window will open.

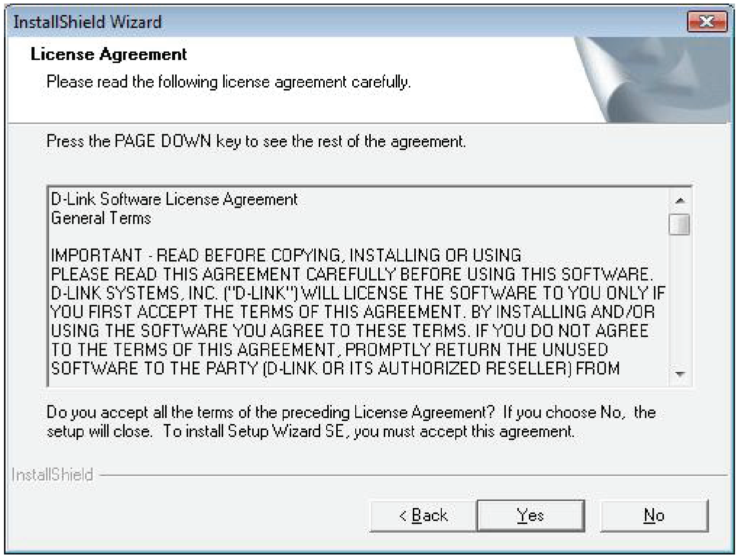
Click **Next** to continue.



Welcome to the InstallShield Wizard for Setup Wizard SE

The InstallShield® Wizard will install Setup Wizard SE on your computer. To continue, click Next.

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



InstallShield Wizard

License Agreement

Please read the following license agreement carefully.

Press the PAGE DOWN key to see the rest of the agreement.

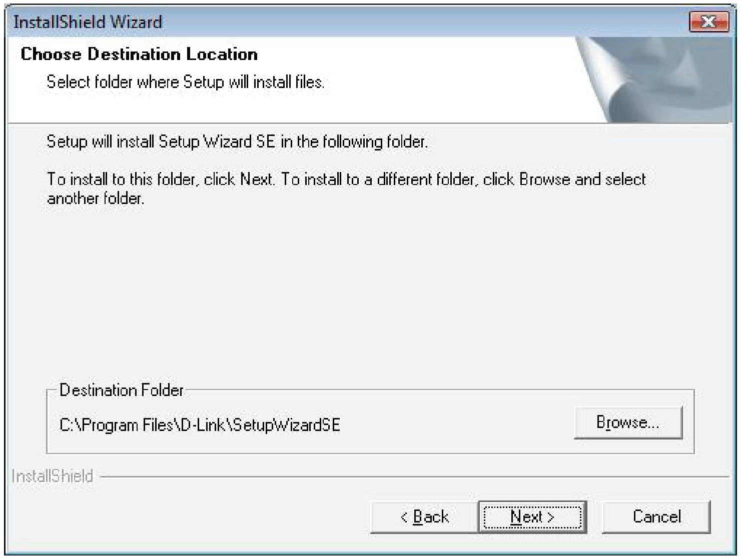
D-Link Software License Agreement
General Terms

IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING
PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS SOFTWARE. D-LINK SYSTEMS, INC. ("D-LINK") WILL LICENSE THE SOFTWARE TO YOU ONLY IF YOU FIRST ACCEPT THE TERMS OF THIS AGREEMENT. BY INSTALLING AND/OR USING THE SOFTWARE YOU AGREE TO THESE TERMS. IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, PROMPTLY RETURN THE UNUSED SOFTWARE TO THE PARTY (D-LINK OR ITS AUTHORIZED RESELLER) FROM

Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install Setup Wizard SE, you must accept this agreement.

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

***Note:** The installation may take several minutes to finish.*



InstallShield Wizard

Choose Destination Location

Select folder where Setup will install files.

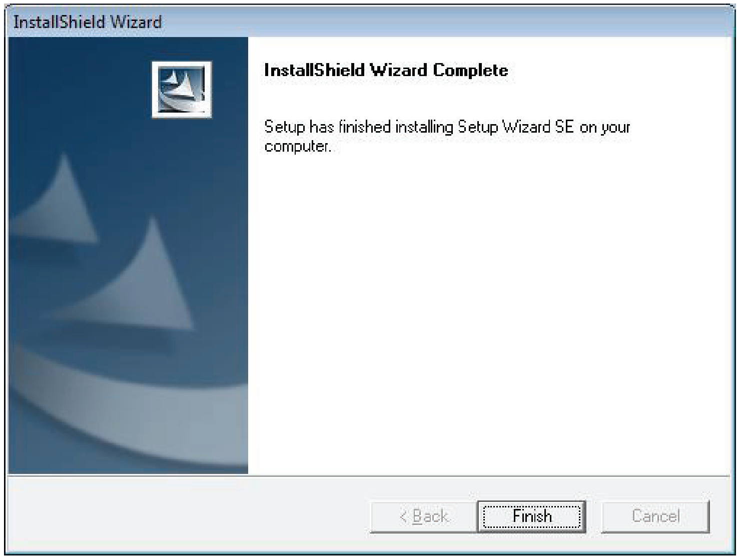
Setup will install Setup Wizard SE in the following folder.

To install to this folder, click Next. To install to a different folder, click Browse and select another folder.

Destination Folder

C:\Program Files\D-Link\SetupWizardSE

Click **Finish** to complete the installation.



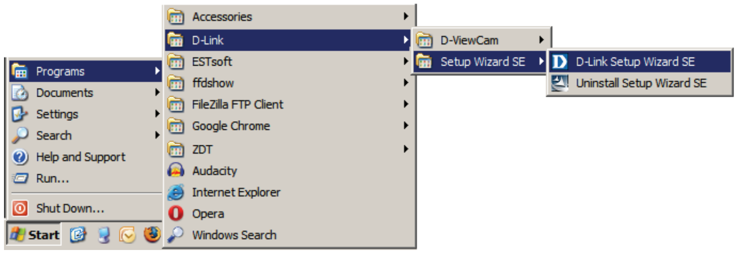
InstallShield Wizard

**InstallShield Wizard Complete**

Setup has finished installing Setup Wizard SE on your computer.

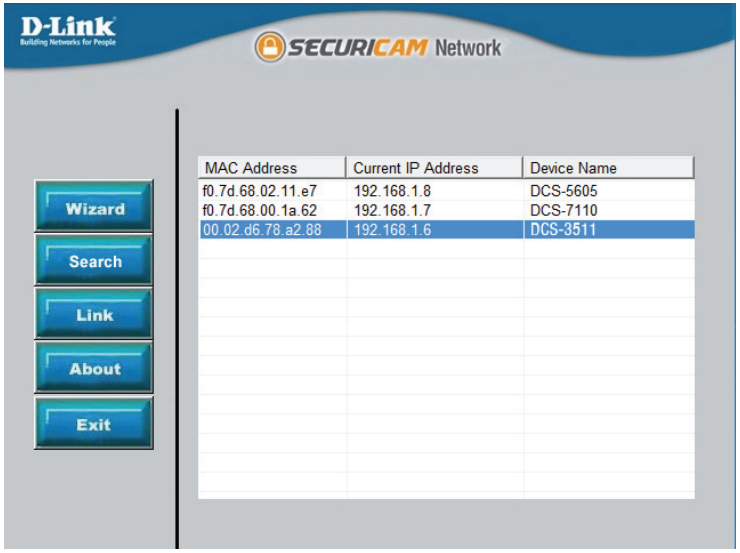
Click on the **D-Link Setup Wizard SE** icon that was created in your Windows Start menu.

**Start** > **D-Link** > **Setup Wizard SE**



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.

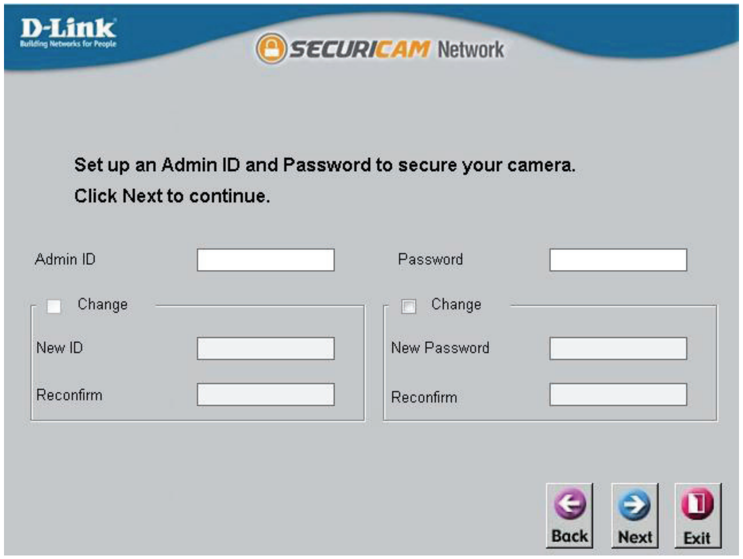
Click the **Wizard** button to continue.



| MAC Address | Current IP Address | Device Name |
|---|---|---|
| f0.7d.68.02.11.e7 | 192.168.1.8 | DCS-5605 |
| f0.7d.68.00.1a.62 | 192.168.1.7 | DCS-7110 |
| 00.02.d6.78.a2.88 | 192.168.1.6 | DCS-3511 |

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.



Set up an Admin ID and Password to secure your camera.
Click Next to continue.

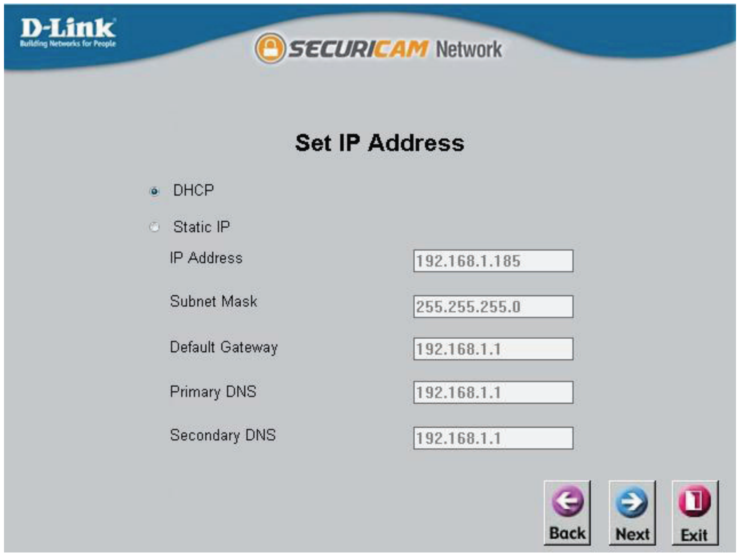
Admin ID ______ Password ______

□ Change
New ID ______
Reconfirm ______

□ Change
New Password ______
Reconfirm ______

Select **DHCP** if you want the camera to obtain an IP address automatically from your router or DHCP server or select **Static IP** to manually assign the camera"s IP settings.

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



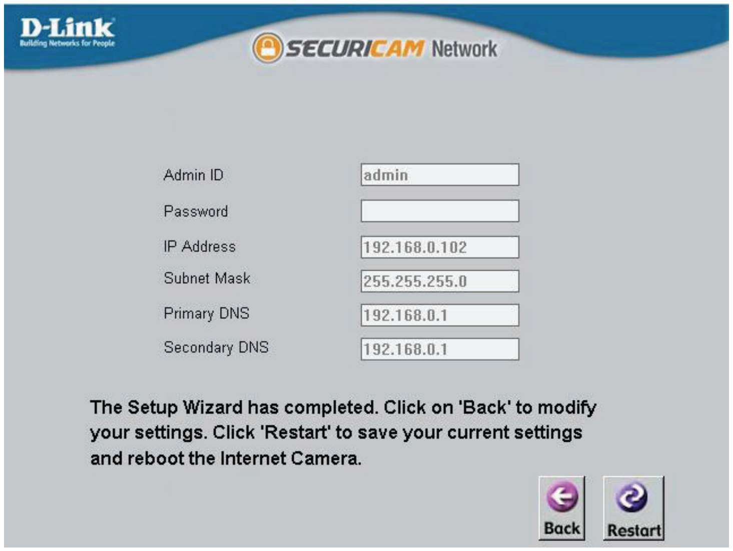
Set IP Address

● 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 |

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



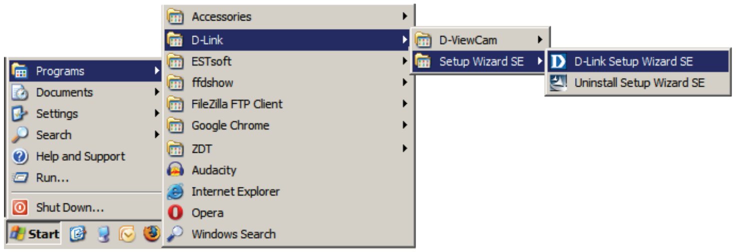
|  |  |
|---|---|
| Admin ID | admin |
| Password |  |
| IP Address | 192.168.0.102 |
| Subnet Mask | 255.255.255.0 |
| Primary DNS | 192.168.0.1 |
| Secondary DNS | 192.168.0.1 |

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

# Viewing Camera via Web Browser

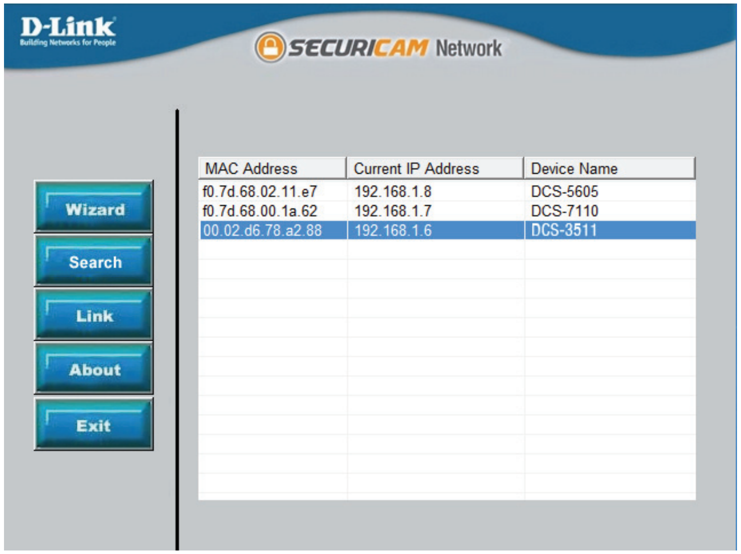
Click on the **D-Link Setup Wizard SE** icon that was created in your Windows Start menu.

**Start** > **D-Link** > **Setup Wizard SE**



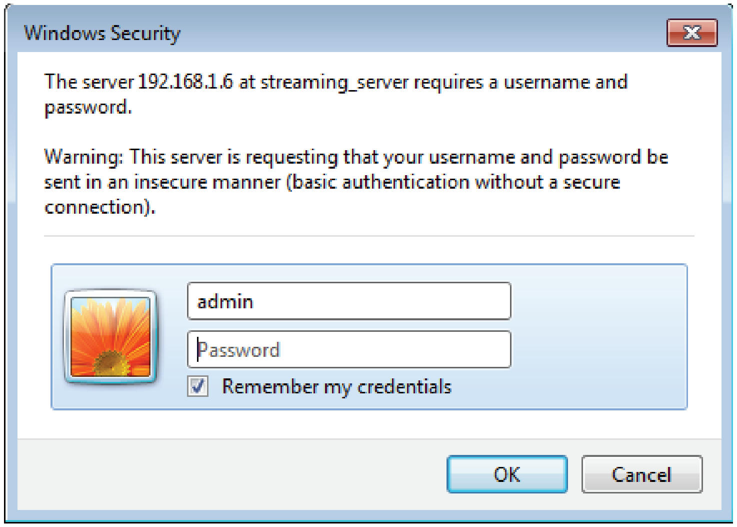
Select the camera and click the button labeled "**Link**" to access the web configuration.

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



| MAC Address | Current IP Address | Device Name |
|---|---|---|
| f0.7d.68.02.11.e7 | 192.168.1.8 | DCS-5605 |
| f0.7d.68.00.1a.62 | 192.168.1.7 | DCS-7110 |
| 00.02.d6.78.a2.88 | 192.168.1.6 | DCS-3511 |

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



Windows Security

The server 192.168.1.6 at streaming_server requires a username and password.

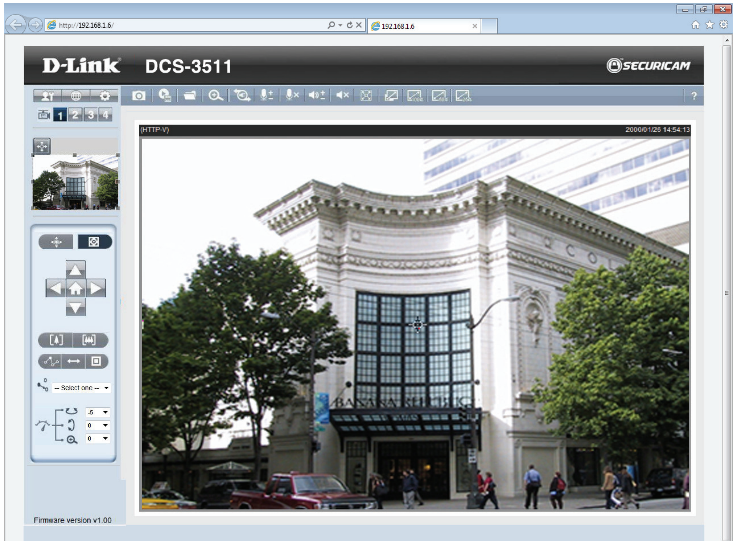
Warning: This server is requesting that your username and password be sent in an insecure manner (basic authentication without a secure connection).

admin

Password

☑ Remember my credentials

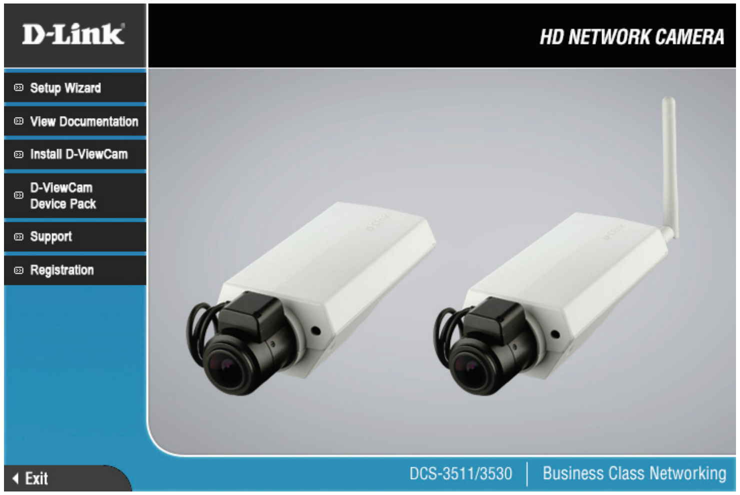
This section shows your camera's live video. You can select your video profile and view or operate the camera.



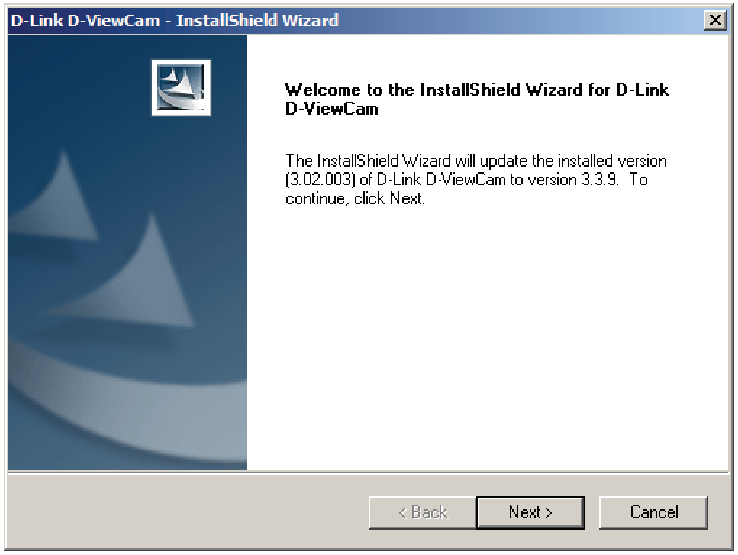
# D-ViewCam Setup Wizard

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. Click Install D-ViewCam and then click the Install button.



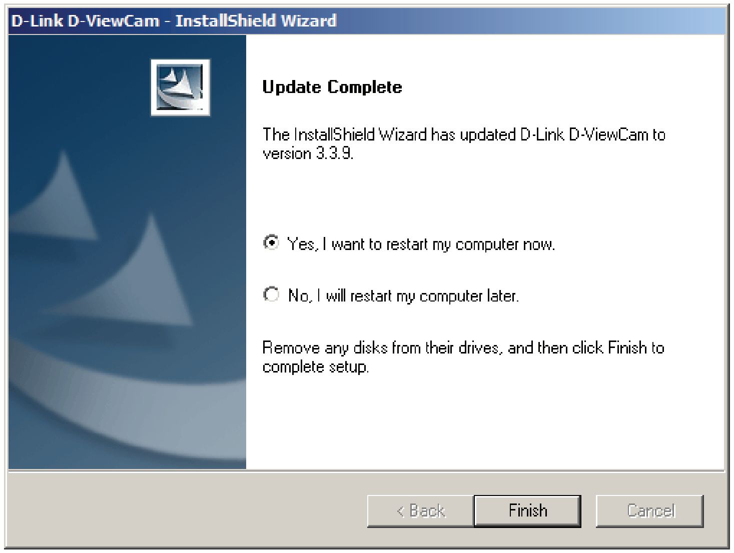
Follow the Installation Wizard to install D-ViewCam.



**Welcome to the InstallShield Wizard for D-Link D-ViewCam**

The InstallShield Wizard will update the installed version (3.02.003) of D-Link D-ViewCam to version 3.3.9. To continue, click Next.

Click **Finish** to complete the installation.



D-Link D-ViewCam - InstallShield Wizard

**Update Complete**

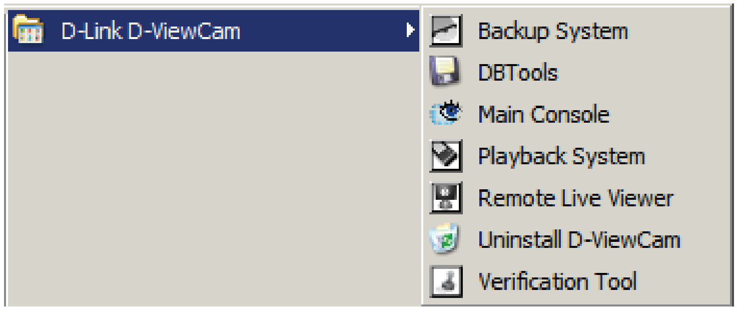
The InstallShield Wizard has updated D-Link D-ViewCam to version 3.3.9.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

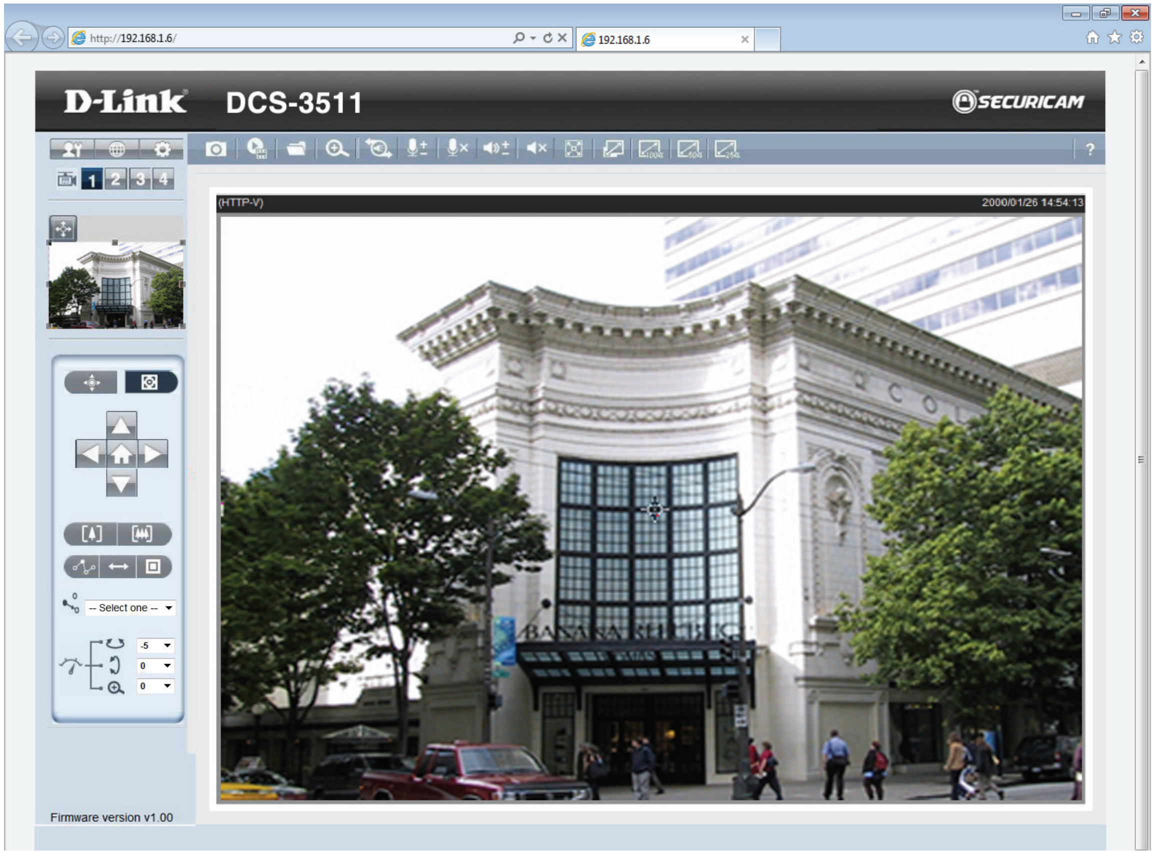
Remove any disks from their drives, and then click Finish to complete setup.

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

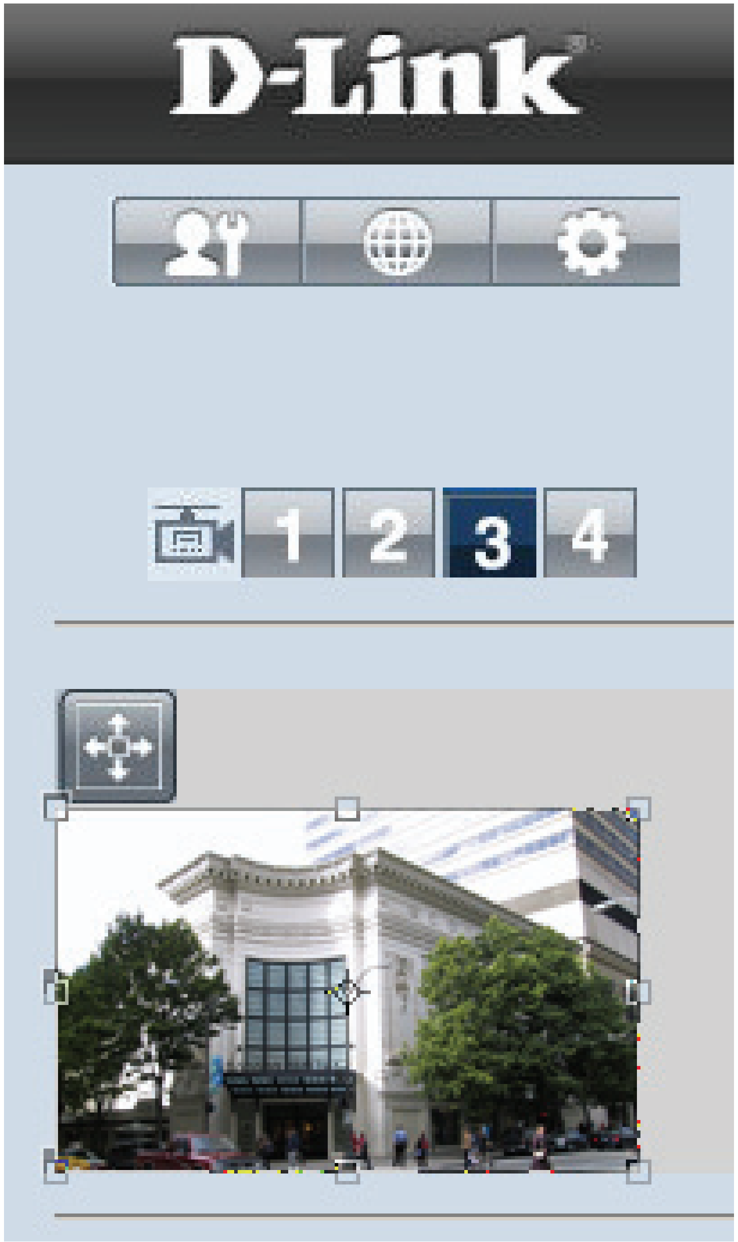


# Live Video

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.

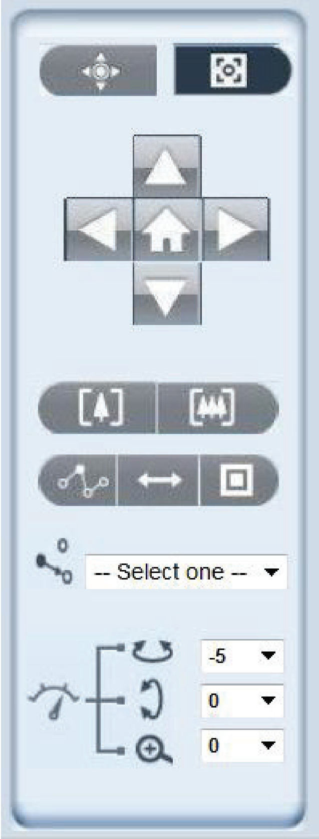


| | |
|---|---|
| D-Link Logo<br>Securicam Logo | Click this logo to visit the D-Link website.<br>The logos and website can be customized to fit your needs. For more information, please refer to User Customization on page <?>. |
| Client Settings | Setup the stream transmission mode and saving options on the local computer. |
| Language | Select this option to adjust the language settings. |
| Setup | Click on the setup icon on the main page to enter the camera setting pages. Note that only Administrators can access the setup page.<br>To simplify the setting procedure, two types of user interfaces are available: **Advanced Setup** for professional users and **Basic Setup** for entry-level users. |
| 1 2 3 4<br>Video Stream | This camera supports multiple streams (stream 1 ~ 4) simultaneously. You may select one for live viewing. |
| Global View | 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. |

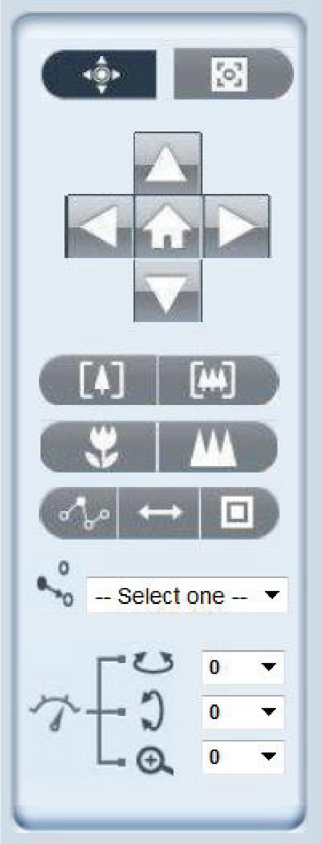


| | |
|---|---|
| PTZ Control | This camera supports both “digital“ (e-PTZ) and “mechanical“ pan/tilt/zoom control. Please refer to PTZ Control for detailed information.<br>**Mechanical PTZ:** Connect the camera to a PTZ driver or scanner via RS-485 interface.<br>**Digital PTZ:** Control the e-PTZ operation. It allows users to quickly move the focus to a target area for close-up viewing without physically moving the camera. |
| ePT Direction | **Home:** Move the camera to the preset home position.<br>**Direction:** Control the camera’s pan or tilt directions (up/down/left/right). |
| Focus | Control camera focus to get a clear image. (Available only under mechanical PTZ mode*)<br>**Focus Near** **Focus Far** |
| Zoom | Zoom in/out to magnify or shrink the digital image.<br>**Zoom in:** Magnify image<br>**Zoom out:** Diminish image |
| Patrol Auto Pan | **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.<br>**Auto Pan:** Auto Pan automatically scans an area horizontally.<br>**Stop:** Stop patrol or auto pan. |
| Go Preset | Select from the preset drop-down list to quickly move the camera to the desired preset position. |
| Speed Control | Control Pan/Tilt/Zoom speed<br>**Pan Speed Control**<br>**Tilt Speed Control**<br>**Zoom Speed Control** |

**Digital PTZ Control Panel**



**Mechanical PTZ Control Panel**



# Camera Control

| | |
|---|---|
| **Snapshot** | 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. |
| **Recording** | Click this button to record video clips to your computer. When you exit the web browser, video recording stops accordingly. |
| **Recording Folder** | Specify a storage destination for the recorded video files. |
| **Digital Zoom** | 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. |
| **Two way audio** | 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. |
| **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. |
| **Microphone Mute** | Click to turn off the microphone (internal/external) that is connected to your network camera. Press again to turn the microphone back on. |
| **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. |
| **Speaker Mute** | Click to mute the external speaker that is connected to the network camera. Press again to un-mute the speaker. |
| **Full Screen** | Click this button to switch to full screen mode. Press the "Esc" key to switch back to normal mode. |
| **Zoom ratio** | **Auto:** The video zoom ratio will be changed automatically according to viewing window size.<br>**100%:** Keep the video zoom ratio at 100%<br>**50%:** Keep the video zoom ratio at 50%<br>**25%:** Keep the video zoom ratio at 25% |
| **Help** | Click the Help button to learn the detailed information regarding camera setup and solve any problems you encounter. |

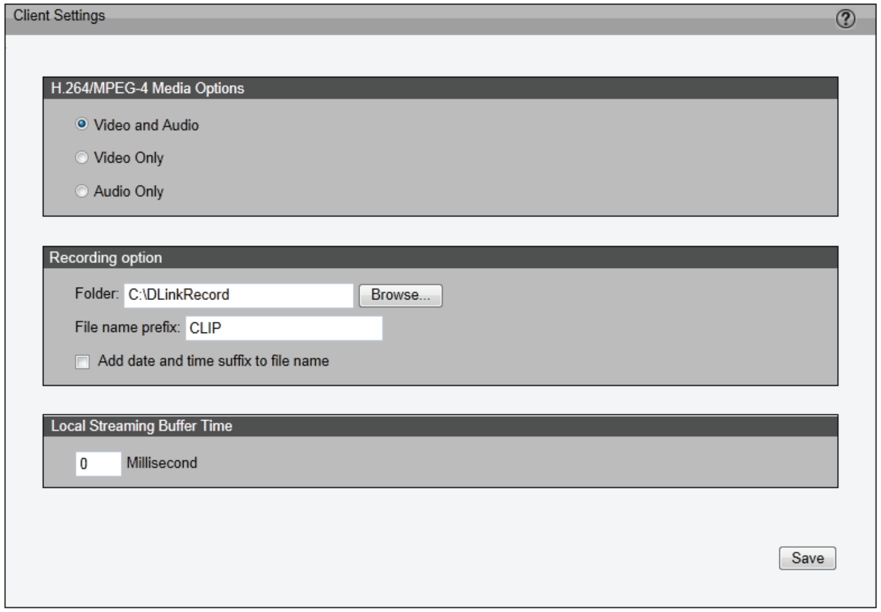
# Client Setup

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 will increase the quality of video.



Client Settings

H.264/MPEG-4 Media Options

● Video and Audio
○ Video Only
○ Audio Only

Recording option

Folder: C:\DLinkRecord
File name prefix: CLIP
□ Add date and time suffix to file name

Local Streaming Buffer Time

0 Millisecond

# 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.

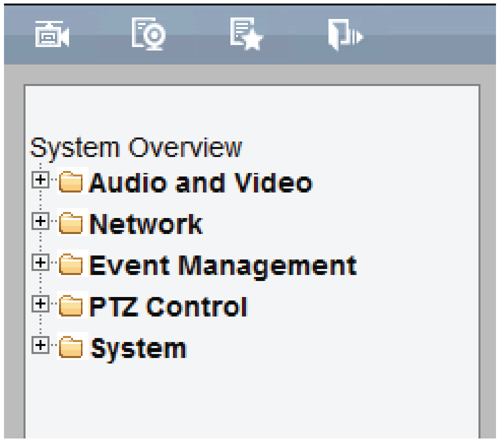
## Standard Setup

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

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

Click the [+] next to each folder to view the options.

Basic setup includes the following options:



System Overview
⊞ Audio and Video
⊞ Network
⊞ Event Management
⊞ PTZ Control
⊞ System

**System Overview**
**Audio and Video**
- Video Settings, Audio Settings, and Day and Night Settings
**Network**
- IP Settings and Wireless Settings (DCS-3530 only)
**Event Management**
- Motion Detection, Tamper Detection, and DI and DO
**PTZ Control**
- Digital PTZ and Mechanical PTZ.
**System**
- User Settings, Device Settings, Time and Date, and Maintenance

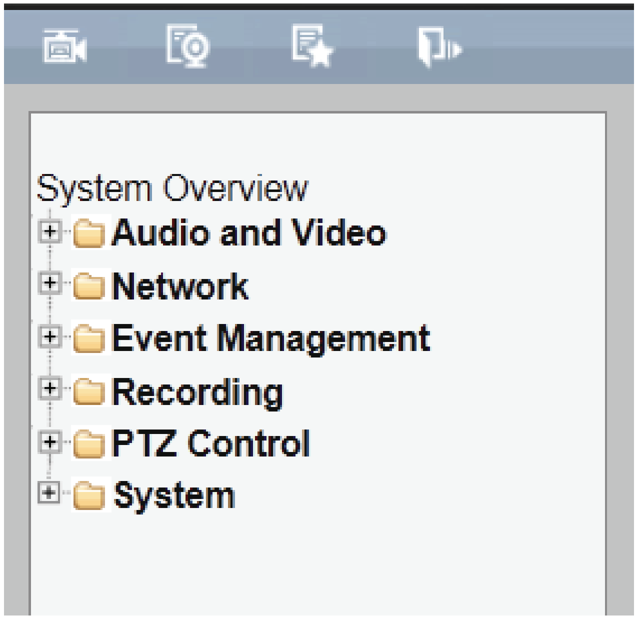
# Advanced Setup

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

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

Click the [+] next to each folder to view the options.

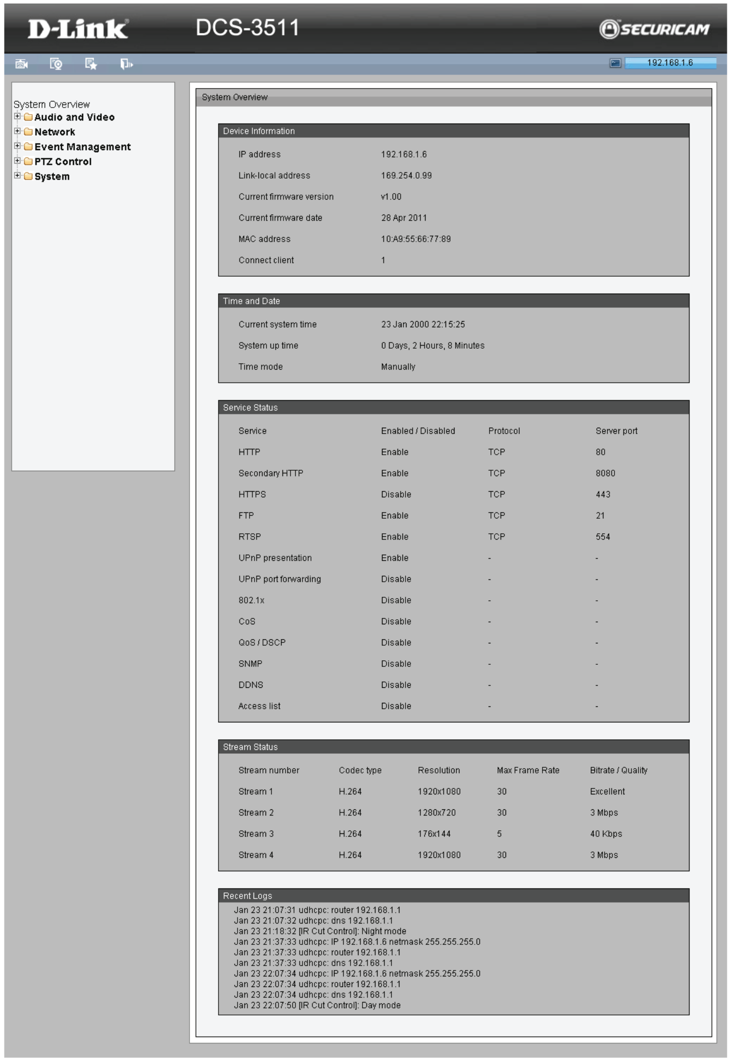
Advanced setup includes the following options:



**System Overview**
**Audio and Video**
- Video Settings, Image Settings, Audio Settings, and Day and Night Settings
**Network**
- IP Settings, Wireless Settings (DCS-3530 only), Port & Access Name Settings, and Dynamic DNS,
HTTPS, Access List, and Advanced Settings
**Event Management**
- Motion Detection, Tamper Detection, DI and DO, and Event Settings
**Recording**
- Recording Settings and Local Storage
**PTZ Control**
- Digtal PTZ and Mechanical PTZ
**System**
- User Settings, Device Settings, Time and Date, Maintenance,
Parameter List, and Logs

# System Overview

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



System Overview

Device Information

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

# Video

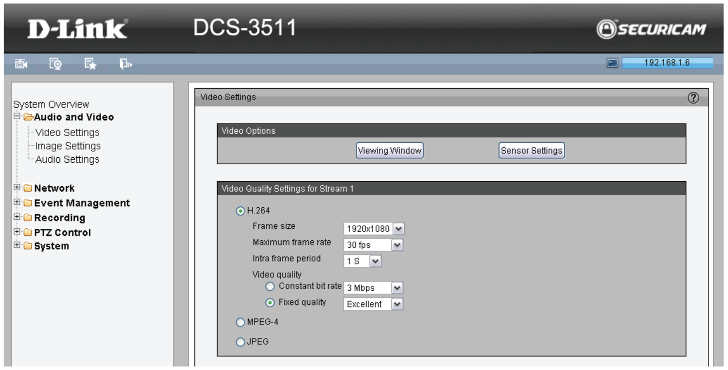
## Video Settings

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.



Video Quality Settings for Stream 1

● H.264

Frame size: 1920x1080

Maximum frame rate: 30 fps

Intra frame period: 1 S

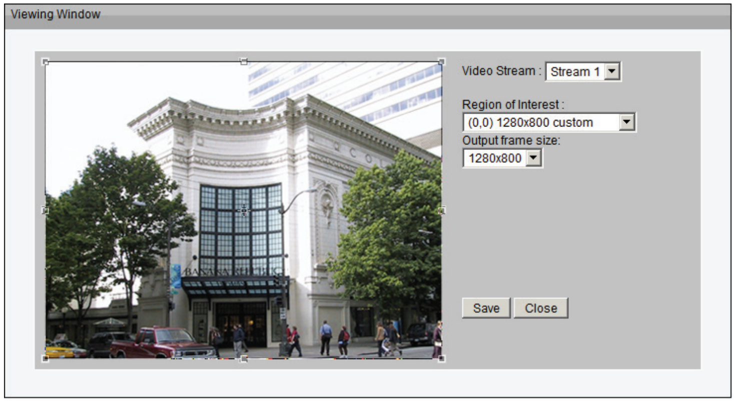
Video quality

○ Constant bit rate: 3 Mbps

● Fixed quality: Excellent

○ MPEG-4

○ JPEG



Viewing Window

Video Stream : Stream 1

Region of Interest : (0,0) 1280x800 custom

Output frame size: 1280x800

***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.

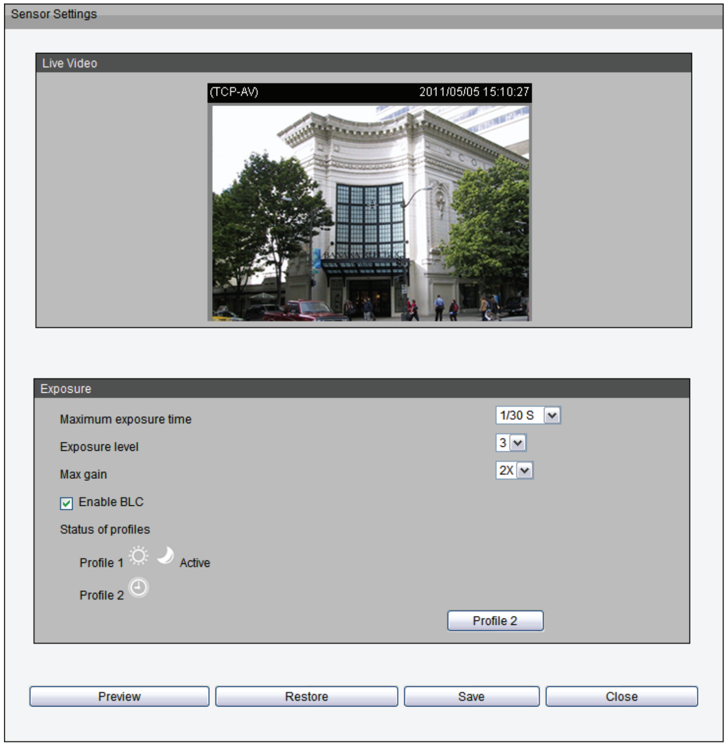
**Sensor Setting:** Click **Sensor Setting** to open the Sensor Setting page. On this page, you can set the maximum exposure time, exposure level, and AGC (Auto Gain Control) setting. You can configure two sets of sensor setting: one for normal situations (Profile 1), the other for special situations, 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: 1/5,1/15,1/30,1/60,1/120,1/240,1/480.
- **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 selected Schedule mode.
3. Configure Exposure setting and Image setting in the third column.
4. Click **Save** to enable the setting and click **Close** to exit the page.


Sensor Settings

Live Video

(TCP-AV) 2011/05/05 15:10:27

Exposure

Maximum exposure time: 1/30 S

Exposure level: 3

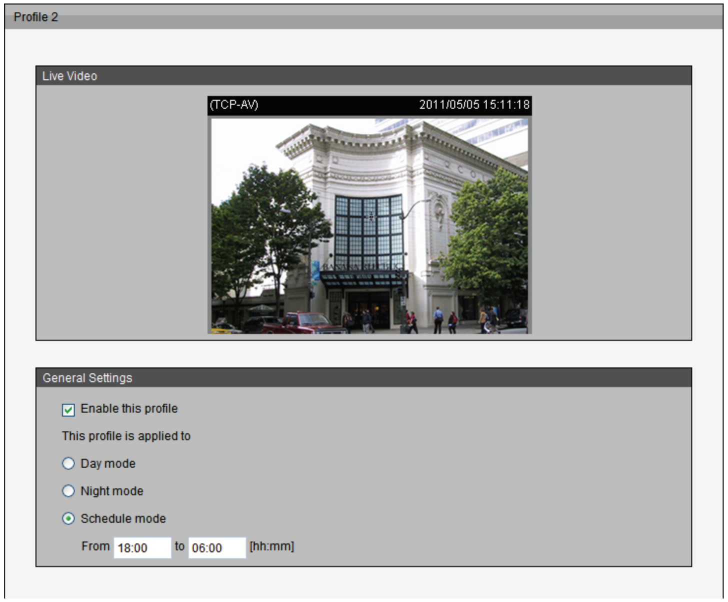
Max gain: 2X

☑ Enable BLC

Status of profiles

Profile 1 Active

Profile 2


Profile 2

Live Video

(TCP-AV) 2011/05/05 15:11:18

General Settings

☑ Enable this profile

This profile is applied to

○ Day mode

○ Night mode

● Schedule mode

From 18:00 to 06:00 [hh:mm]

### Video Quality Setting for Stream 1~4

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

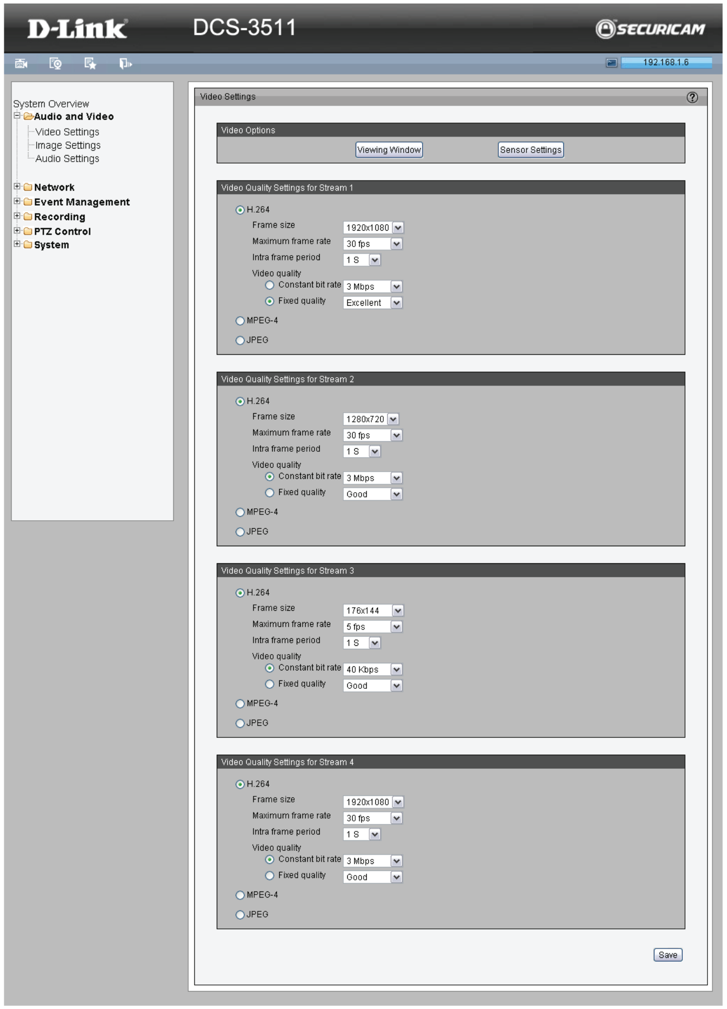
**Frame Size:** Select proper frame size for different viewing devices, bigger frame size requires more bandwidth, and storage usage. For smaller viewers, such as mobile phones, a smaller frame size and lower frame rate is recommended. There are 5 options you can select: 176x144, 320x240, 640x480, 1280x720, 1280x800.

**Frame Rate:** This option affects the smoothness of the video. Select higher frame rate for smoother video quality but it requires more storage usage. Ten 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 of the Iframe.  The shorter the duration, the more likely you will get better video quality, but at the cost of higher network bandwidth consumption. Select the intra frame period from the following durations: 1/4 second, 1/2 second, 1 second, 2 seconds, 3 seconds and 4 seconds.

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

- **Constant bit rate:** To set a fixed bandwidth regardless of the video quality, select Constant bit rate and the desired bandwidth from 20 Kbps to 8 Mbps.
- **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.



Video Quality Settings for Stream 1
● H.264
Frame size: 1920x1080
Maximum frame rate: 30 fps
Intra frame period: 1 S
Video quality
○ Constant bit rate: 3 Mbps
● Fixed quality: Excellent
○ MPEG-4
○ JPEG

Video Quality Settings for Stream 2
● H.264
Frame size: 1280x720
Maximum frame rate: 30 fps
Intra frame period: 1 S
Video quality
● Constant bit rate: 3 Mbps
○ Fixed quality: Good
○ MPEG-4
○ JPEG

Video Quality Settings for Stream 3
● H.264
Frame size: 176x144
Maximum frame rate: 5 fps
Intra frame period: 1 S
Video quality
● Constant bit rate: 40 Kbps
○ Fixed quality: Good
○ MPEG-4
○ JPEG

Video Quality Settings for Stream 4
● H.264
Frame size: 1920x1080
Maximum frame rate: 30 fps
Intra frame period: 1 S
Video quality
● Constant bit rate: 3 Mbps
○ Fixed quality: Good
○ MPEG-4
○ JPEG

# Image Settings

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

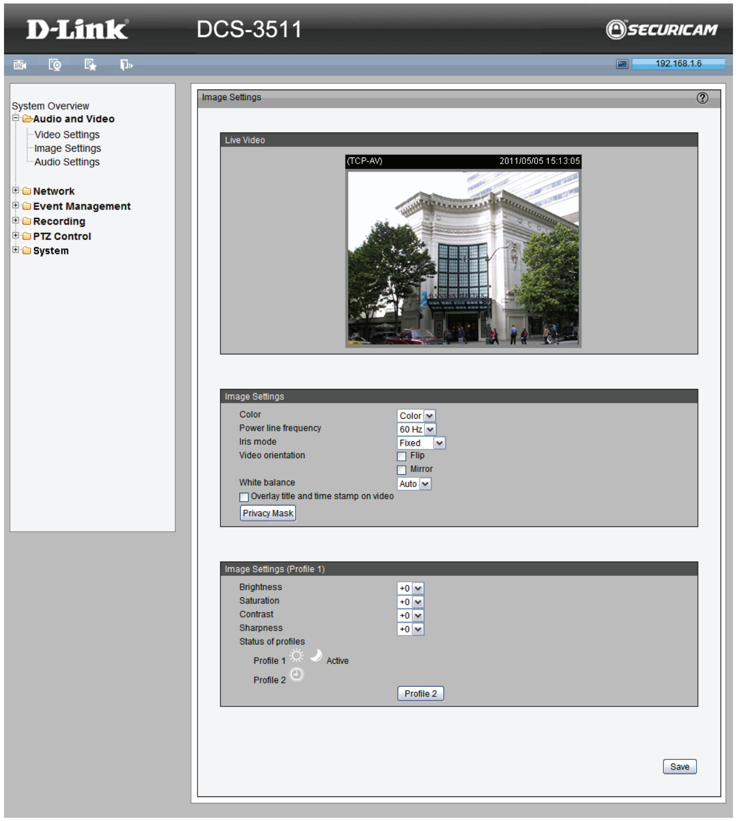


Image Settings

| | |
|---|---|
| Color | Color |
| Power line frequency | 60 Hz |
| Iris mode | Fixed |
| Video orientation | □ Flip |
| | □ Mirror |
| White balance | Auto |

□ Overlay title and time stamp on video

Privacy Mask

Image Settings (Profile 1)

| | |
|---|---|
| Brightness | +0 |
| Saturation | +0 |
| Contrast | +0 |
| Sharpness | +0 |

Status of profiles

Profile 1 Active

Profile 2

Profile 2

Save

**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, or 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. Note when the frame size is set to 176 x 144 only the time will be stamped on the video streams.

**Note:**

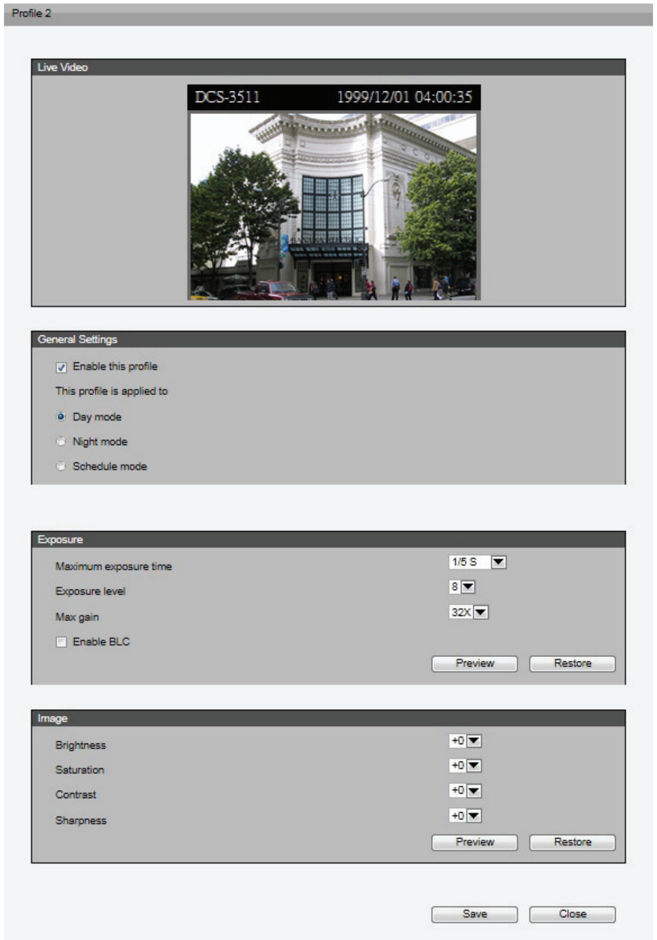
- The "Sensor Settings" and "Image Settings" share the same Profile 2 settings.

**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.



Profile 2

Live Video

DCS-3511 1999/12/01 04:00:35

General Settings

☑ Enable this profile

This profile is applied to

● Day mode

○ Night mode

○ Schedule mode

Exposure

Maximum exposure time 1/5 S

Exposure level 8

Max gain 32X

□ Enable BLC

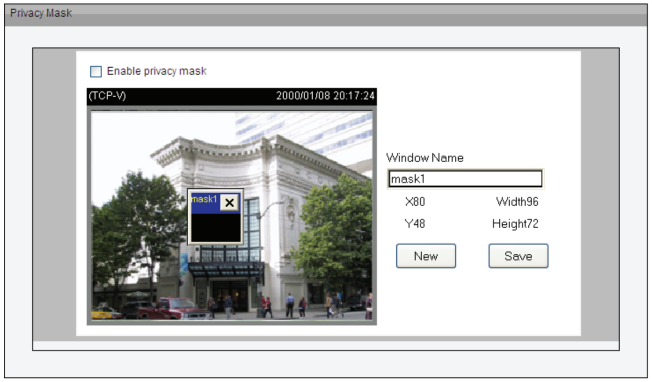
Image

Brightness +0

Saturation +0

Contrast +0

Sharpness +0



Privacy Mask

□ Enable privacy mask

(TCP-V) 2000/01/08 20:17:24

Window Name mask1

X80 Width96

Y48 Height72

# Audio Settings

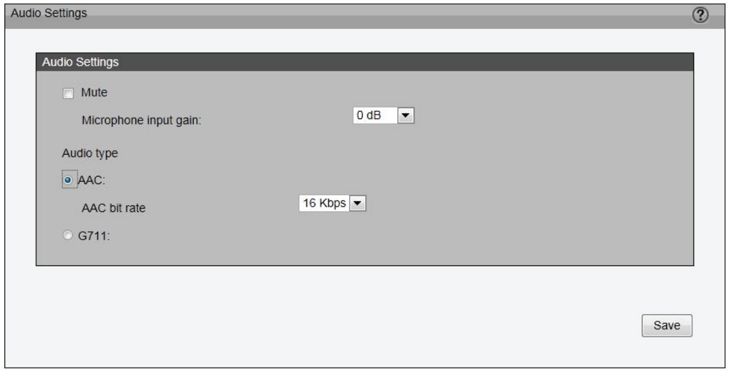
**Mute:** Select to mute audio.

**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.



Audio Settings

Audio Settings

□ Mute

Microphone input gain: 0 dB

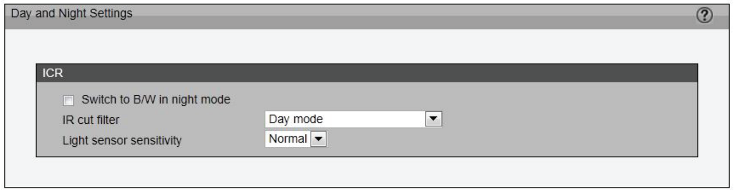
Audio type

● AAC:

AAC bit rate: 16 Kbps

○ G711:

# Day and Night Settings



Day and Night Settings

ICR

□ Switch to B/W in night mode

IR cut filter: Day mode

Light sensor sensitivity: Normal

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

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

- **Auto Mode:** The camera automatically switches between day and night mode by judging the level of ambient light. This mode is accessible only when the exposure mode is set to **Auto**.

- **Day Mode:** In this mode the camera switches on the IR cut filter at all times, which will block the infrared light from reaching the sensor so that the colors are not distorted.

- **Night Mode:** The camera switches off the IR cut filter to allow the infrared light to pass through. This helps the camera to see more clearly in low light conditions.

- **Synchronize with Digital Input:** The camera automatically removes the IR cut filter when DI triggers.

- **Schedule Mode:** The camera switches between day and night mode based on a specific schedule. Ensure to enter the starting and ending time for the day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the starting time and ending time of day mode are set to 07:00 and 18:00.

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

# 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 (i.e., router) 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:** Enter the subnet mask of your network. The default value is "255.255.255.0."

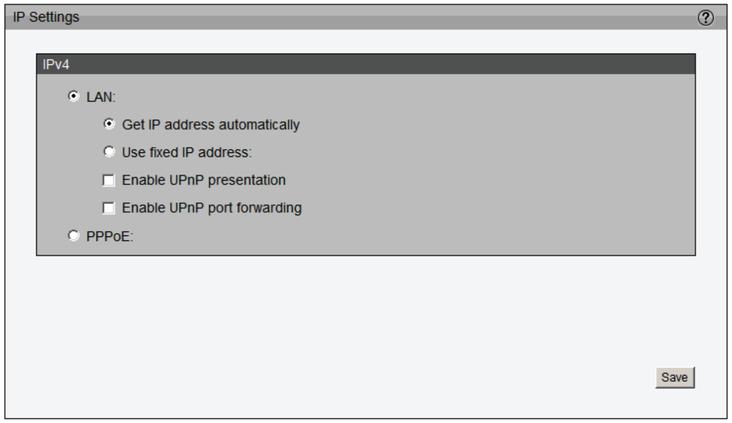
**Default Router:** Enter the default gateway address. This is normally your router's LAN IP address.

**Primary DNS:** Enter the primarty DNS server IP address.

**Secondary DNS:** Enter a secondary DNS server IP address.

**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.



IP Settings

IPv4

● LAN:

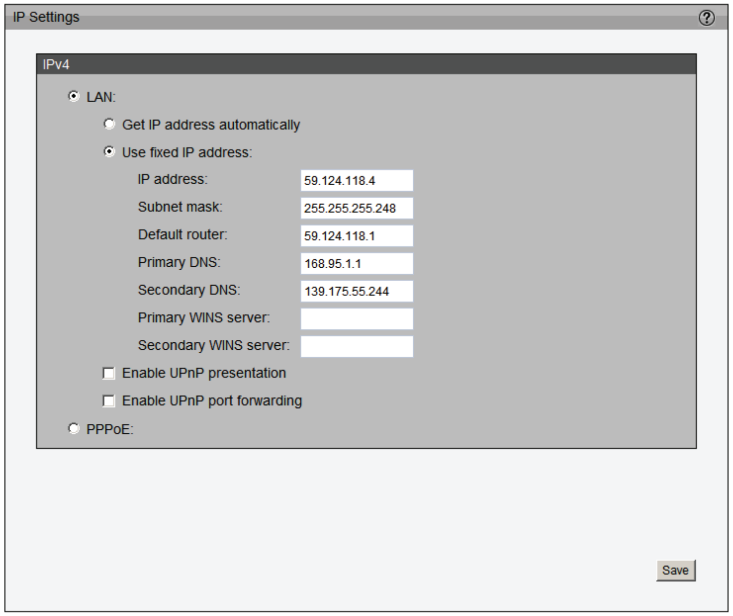
● Get IP address automatically

○ Use fixed IP address:

□ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE:



IP Settings

IPv4

● LAN:

○ Get IP address automatically

● Use fixed IP address:

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

□ Enable UPnP presentation

□ Enable UPnP port forwarding

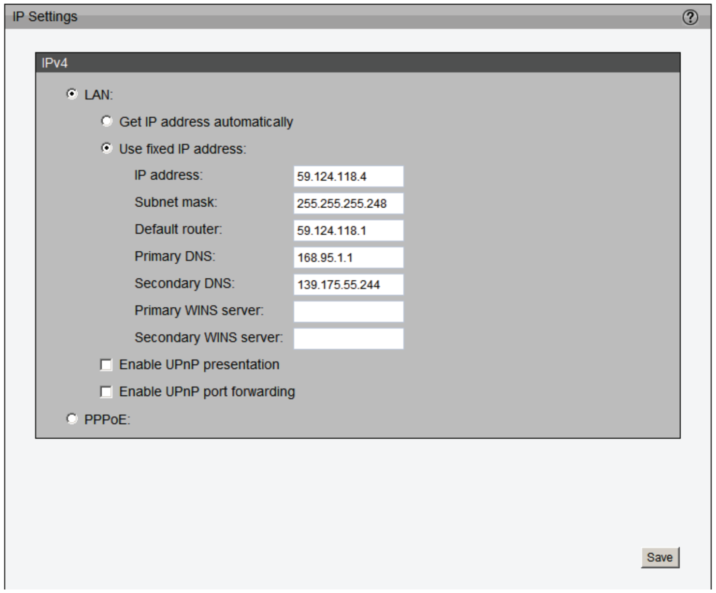
○ PPPoE:

- **Enable UPnP Presentation:** Select this option to enable UPnP presentation for the camera so that whenever a camera is presented to the local network, shortcuts of connected cameras will be listed in My Network Places. You can click the shortcut to link which will open the camera's interface to your web browser.
- **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 your local network. To utilize this feature, make sure that your router supports UPnP and it is enabled.

**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 your local network.
2. Go to **Live View** > **Setup** > **Event management** > **Event settings** > **Server Settings** (refer to Server Settings to add a new e-mail or FTP server).
3. Go to **Setup** > **Event management** > **Event settings** > **Media Settings** (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.


IP Settings

IPv4

● LAN:

○ Get IP address automatically

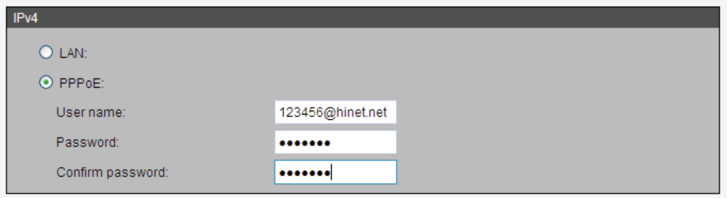
● Use fixed IP address:

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

□ Enable UPnP presentation

□ Enable UPnP port forwarding

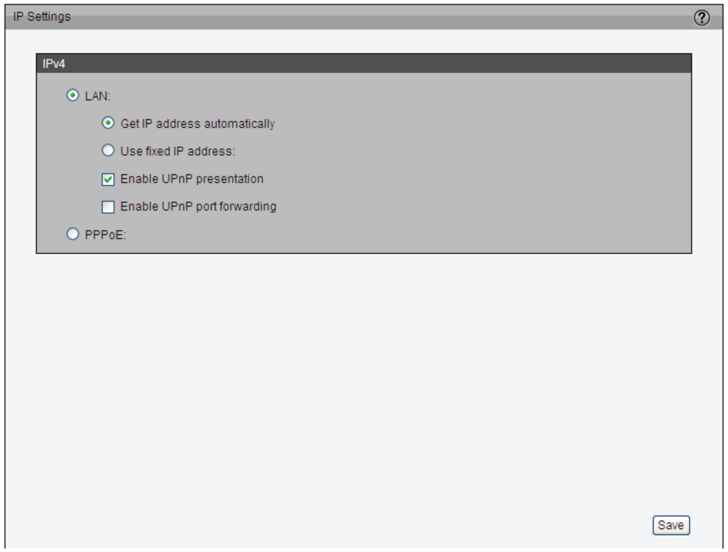
○ PPPoE:


IPv4

○ LAN:

● PPPoE:

| | |
|---|---|
| User name: | 123456@hinet.net |
| Password: | ••••••• |
| Confirm password: | ••••••• |


IP Settings

IPv4

● LAN:

● Get IP address automatically

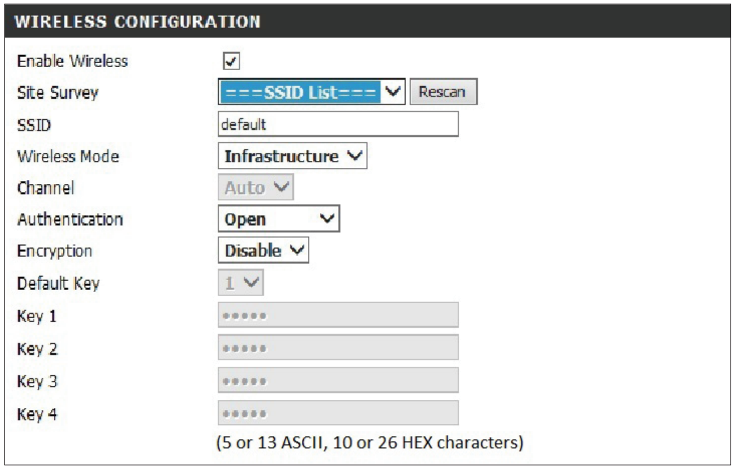
○ Use fixed IP address:

☑ Enable UPnP presentation

□ Enable UPnP port forwarding

○ PPPoE:

# Wireless Settings



WIRELESS CONFIGURATION

| | |
|---|---|
| Enable Wireless | ☑ |
| Site Survey | ===SSID List=== Rescan |
| SSID | default |
| Wireless Mode | Infrastructure |
| Channel | Auto |
| Authentication | Open |
| Encryption | Disable |
| Default Key | 1 |
| Key 1 | ••••• |
| Key 2 | ••••• |
| Key 3 | ••••• |
| Key 4 | ••••• |
| | (5 or 13 ASCII, 10 or 26 HEX characters) |

*** 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 network 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 (most common) is used to connect to an access point or router. Ad-Hoc is usually used to connect directly to another computer (peer to peer).

**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 a passphrase or Wi-Fi password) used for your wireless network.

# 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.

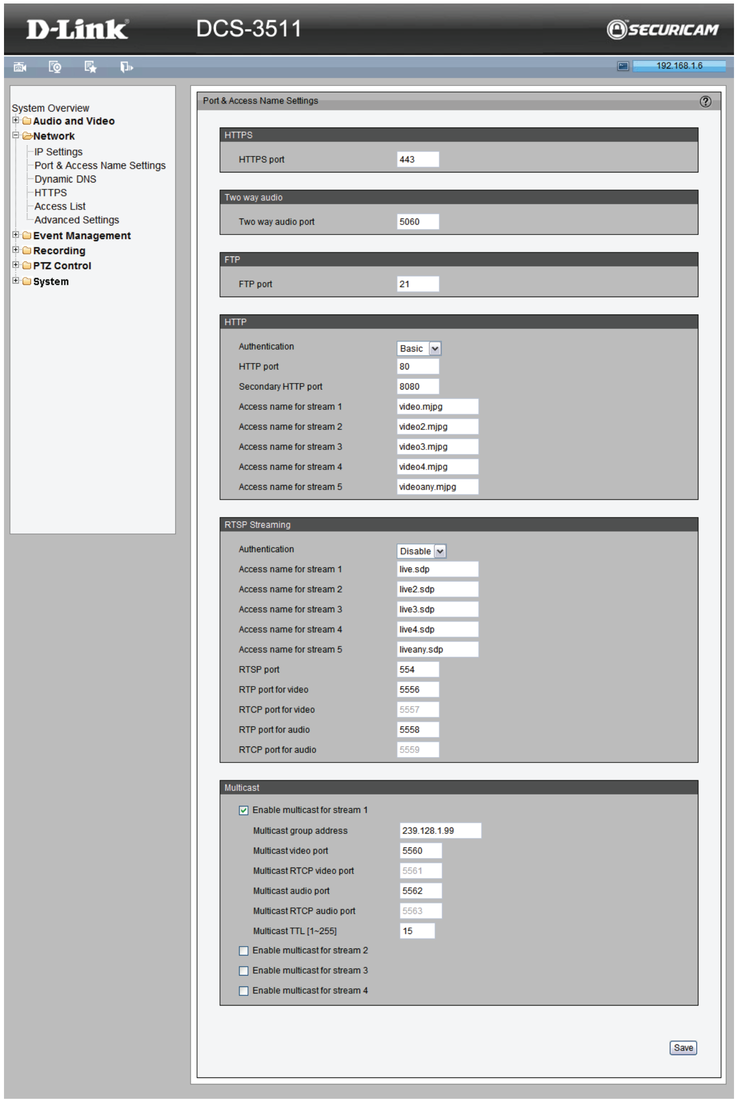
***Note:*** *JPEG only transmits a series of JPEG images to the client. In order to utilize this audio feature, make sure the video mode is set to H.264 or MPEG-4 and the media option in "Client Settings" is set to* ***Video and Audio****.*

**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 log in the 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.



Port & Access Name Settings

HTTPS

| | |
|---|---|
| HTTPS port | 443 |

Two way audio

| | |
|---|---|
| Two way audio port | 5060 |

FTP

| | |
|---|---|
| FTP port | 21 |

HTTP

| | |
|---|---|
| Authentication | Basic |
| HTTP port | 80 |
| Secondary HTTP port | 8080 |
| Access name for stream 1 | video.mjpg |
| Access name for stream 2 | video2.mjpg |
| Access name for stream 3 | video3.mjpg |
| Access name for stream 4 | video4.mjpg |
| Access name for stream 5 | videoany.mjpg |

RTSP Streaming

| | |
|---|---|
| Authentication | Disable |
| Access name for stream 1 | live.sdp |
| Access name for stream 2 | live2.sdp |
| Access name for stream 3 | live3.sdp |
| Access name for stream 4 | live4.sdp |
| Access name for stream 5 | liveany.sdp |
| RTSP port | 554 |
| RTP port for video | 5556 |
| RTCP port for video | 5557 |
| RTP port for audio | 5558 |
| RTCP port for audio | 5559 |

Multicast

☑ Enable multicast for stream 1

| | |
|---|---|
| Multicast group address | 239.128.1.99 |
| Multicast video port | 5560 |
| Multicast RTCP video port | 5561 |
| Multicast audio port | 5562 |
| Multicast RTCP audio port | 5563 |
| Multicast TTL [1~255] | 15 |

☐ Enable multicast for stream 2
☐ Enable multicast for stream 3
☐ Enable multicast for stream 4

When using Firefox 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 Firefox; and use the following HTTP URL command to request transmission of the streaming data.

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

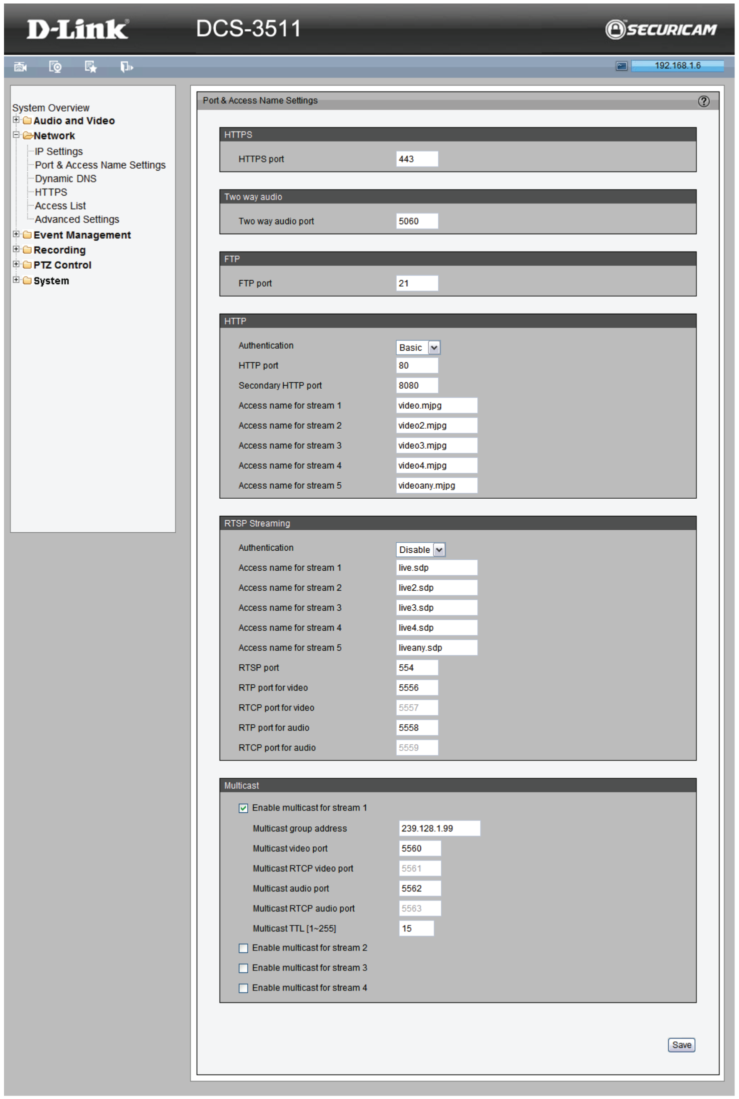
For example, when the Access name for Stream 3 is set to video3.mjpg:
1. Launch Firefox.
2. Type the above URL command in the address bar. Press Enter.
3. The JPEG images will be displayed in your web browser.

***Note:*** *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.



Port & Access Name Settings

HTTPS

| | |
|---|---|
| HTTPS port | 443 |

Two way audio

| | |
|---|---|
| Two way audio port | 5060 |

FTP

| | |
|---|---|
| FTP port | 21 |

HTTP

| | |
|---|---|
| Authentication | Basic |
| HTTP port | 80 |
| Secondary HTTP port | 8080 |
| Access name for stream 1 | video.mjpg |
| Access name for stream 2 | video2.mjpg |
| Access name for stream 3 | video3.mjpg |
| Access name for stream 4 | video4.mjpg |
| Access name for stream 5 | videoany.mjpg |

RTSP Streaming

| | |
|---|---|
| Authentication | Disable |
| Access name for stream 1 | live.sdp |
| Access name for stream 2 | live2.sdp |
| Access name for stream 3 | live3.sdp |
| Access name for stream 4 | live4.sdp |
| Access name for stream 5 | liveany.sdp |
| RTSP port | 554 |
| RTP port for video | 5556 |
| RTCP port for video | 5557 |
| RTP port for audio | 5558 |
| RTCP port for audio | 5559 |

Multicast

☑ Enable multicast for stream 1

| | |
|---|---|
| Multicast group address | 239.128.1.99 |
| Multicast video port | 5560 |
| Multicast RTCP video port | 5561 |
| Multicast audio port | 5562 |
| Multicast RTCP audio port | 5563 |
| Multicast TTL [1~255] | 15 |

☐ Enable multicast for stream 2
☐ Enable multicast for stream 3
☐ Enable multicast for stream 4

**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 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.

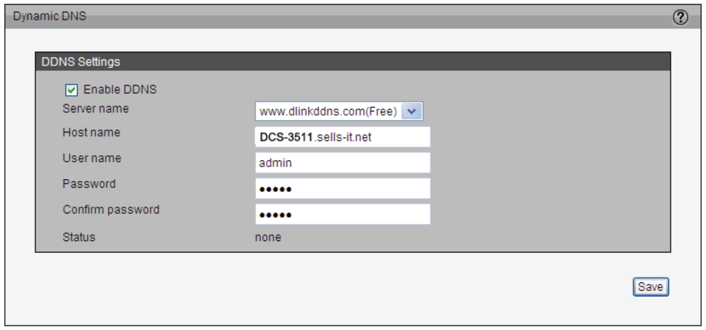
**Multicast:**
Click the items to display the detailed configuration information. Select the **Always Multicast** option to enable multicast for stream 1 ~ 4.
Unicast video transmission delivers a stream through point-to-point transmission; multicast, on the other hand, sends a stream to the multicast 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.



DDNS Settings

☑ Enable DDNS

| | |
|---|---|
| Server name | www.dlinkddns.com(Free) |
| Host name | DCS-3511.sells-it.net |
| User name | admin |
| Password | ••••• |
| Confirm password | ••••• |
| Status | none |

**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:** Displays the current connection status.

# 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 with a 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.

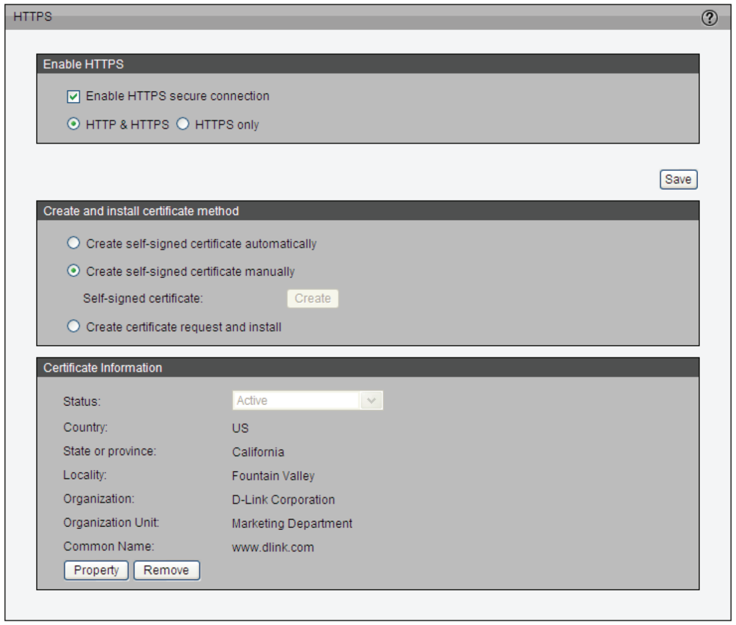
There are three ways to create and install a certificate:

**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.



HTTPS

Enable HTTPS

☑ Enable HTTPS secure connection

● HTTP & HTTPS ○ HTTPS only

Save

Create and install certificate method

○ Create self-signed certificate automatically

● Create self-signed certificate manually

Self-signed certificate: Create

○ Create certificate request and install

Certificate Information

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

Property Remove

### Create Certificate Request and Install

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

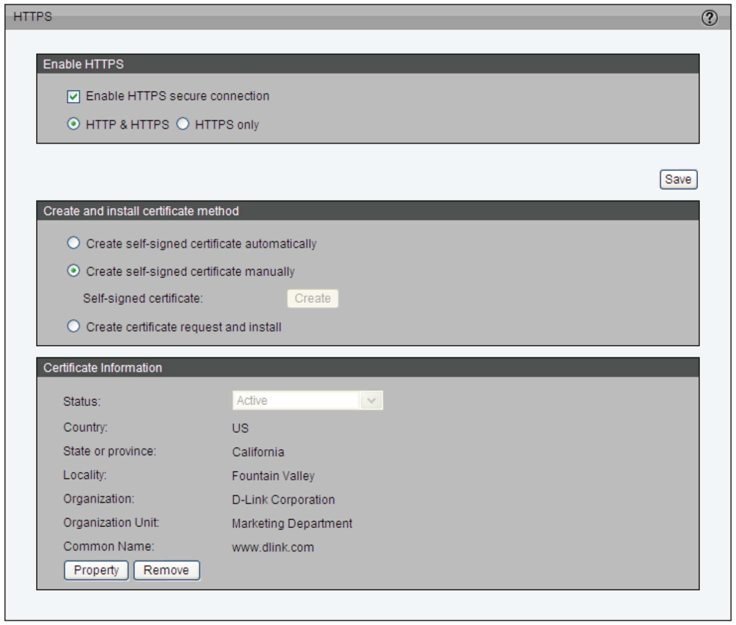
1. Click **Create** to open the **Create Certificate** page, then click **Save** to generate the certificate.
2. If you see the information bar, click **OK** and click on the Information bar at the top of the page to allow pop-up.
3. The pop-up window shows an example of a certificate request.
4. Look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



HTTPS

Enable HTTPS

☑ Enable HTTPS secure connection

● HTTP & HTTPS ○ HTTPS only

Save

Create and install certificate method

○ Create self-signed certificate automatically

● Create self-signed certificate manually

Self-signed certificate: Create

○ Create certificate request and install

Certificate Information

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

Property Remove

# Access List

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

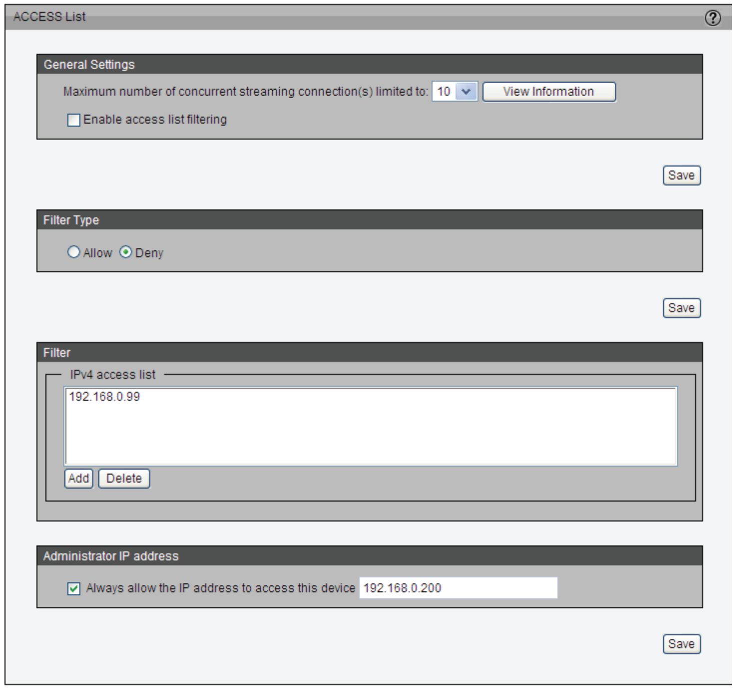
**General Settings**
Maximum number of concurrent streaming connection(s) limited to: Simultaneous live viewing for 1~10 clients (including stream 1 ~ stream 5). The default value is 10. If you modify the value and click **Save**, all current connections will be disconnected and automatically attempt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


ACCESS List

General Settings

Maximum number of concurrent streaming connection(s) limited to: 10

□ Enable access list filtering

Filter Type

○ Allow ● Deny

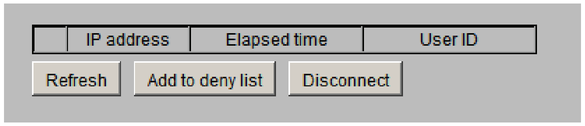
Filter

IPv4 access list

192.168.0.99

Administrator IP address

☑ Always allow the IP address to access this device 192.168.0.200



- **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 (i.e., Explore or Quick Time Player). If you want to enable the denied list, 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 (i.e., 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 select Allow, only those clients whose IP addresses are on the Access List can access the camera. All others will be blocked. If you select Deny, those clients whose IP addresses are on the Access List will not be allowed to access the camera. All others can access.

**Filter**

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:

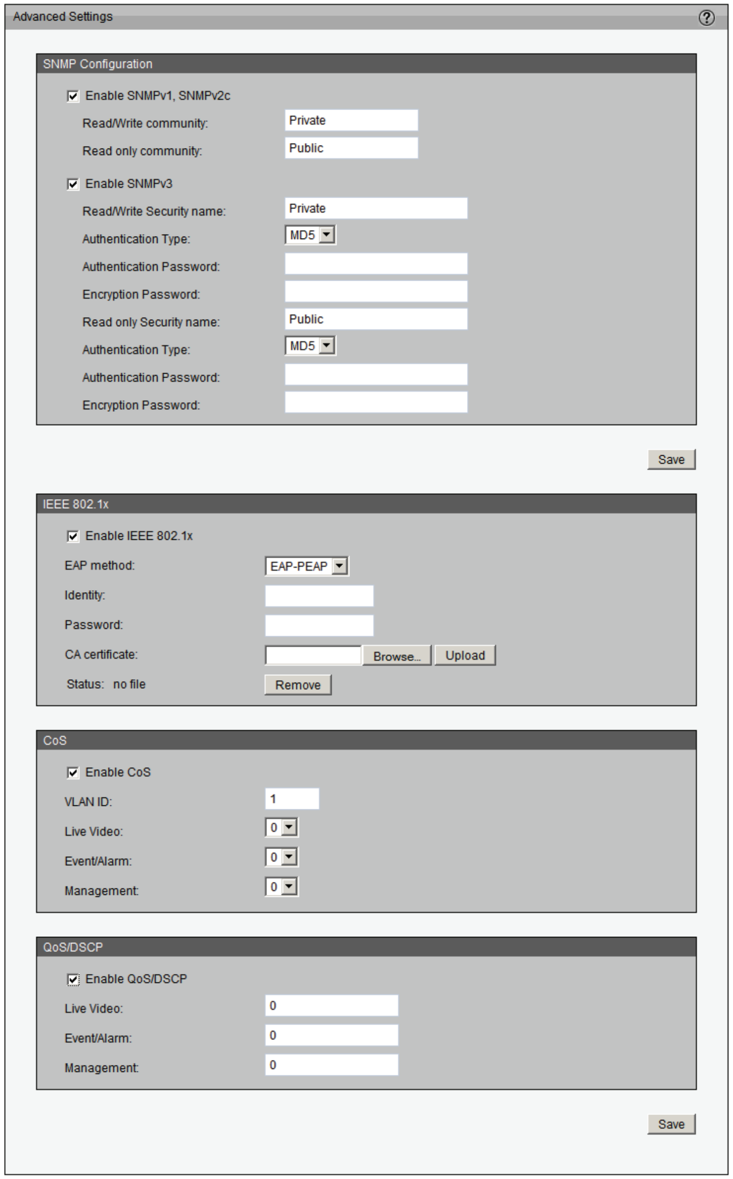
1. **Manager:** Network-Management Station (NMS), a server which executes applications that monitor and control managed devices.
2. **Agent:** A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. **Managed device:** A network node on a 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, 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-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x setting.



Advanced Settings

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: | |
| Encryption Password: | |
| Read only Security name: | Public |
| Authentication Type: | MD5 |
| Authentication Password: | |
| Encryption Password: | |

IEEE 802.1x

☑ Enable IEEE 802.1x

| | |
|---|---|
| EAP method: | EAP-PEAP |
| Identity: | |
| Password: | |
| CA certificate: | |
| Status: no file | |

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 |

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.

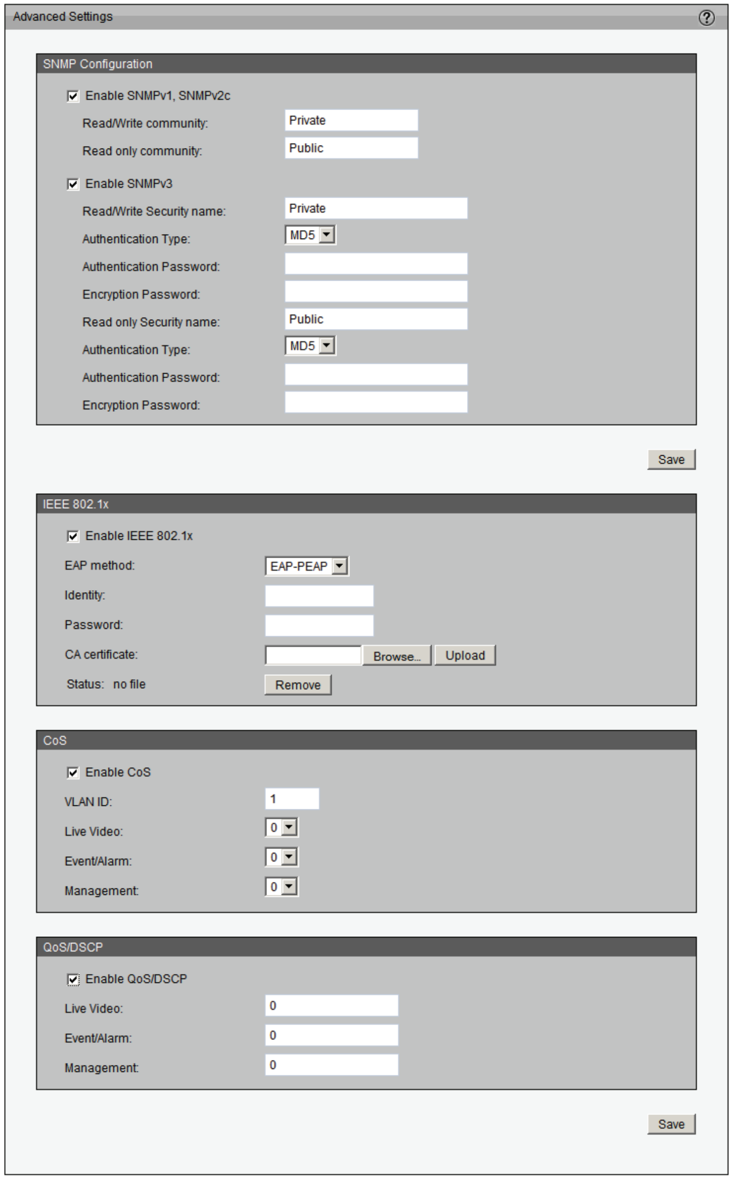
Please follow the steps below to enable 802.1x setting:

1. Before connecting the camera to the protected network with 802.1x, apply a digital certificate from a Certificate Authority (i.e., MIS of your company) which can be validated by a RADIUS server.
2. Connect the camera to a computer 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 fields, 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 provide higher reliability and stability on the network.



Advanced Settings

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:
Encryption Password:
Read only Security name: Public
Authentication Type: MD5
Authentication Password:
Encryption Password:

Save

IEEE 802.1x

☑ Enable IEEE 802.1x

EAP method: EAP-PEAP
Identity:
Password:
CA certificate: 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

Save

**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.

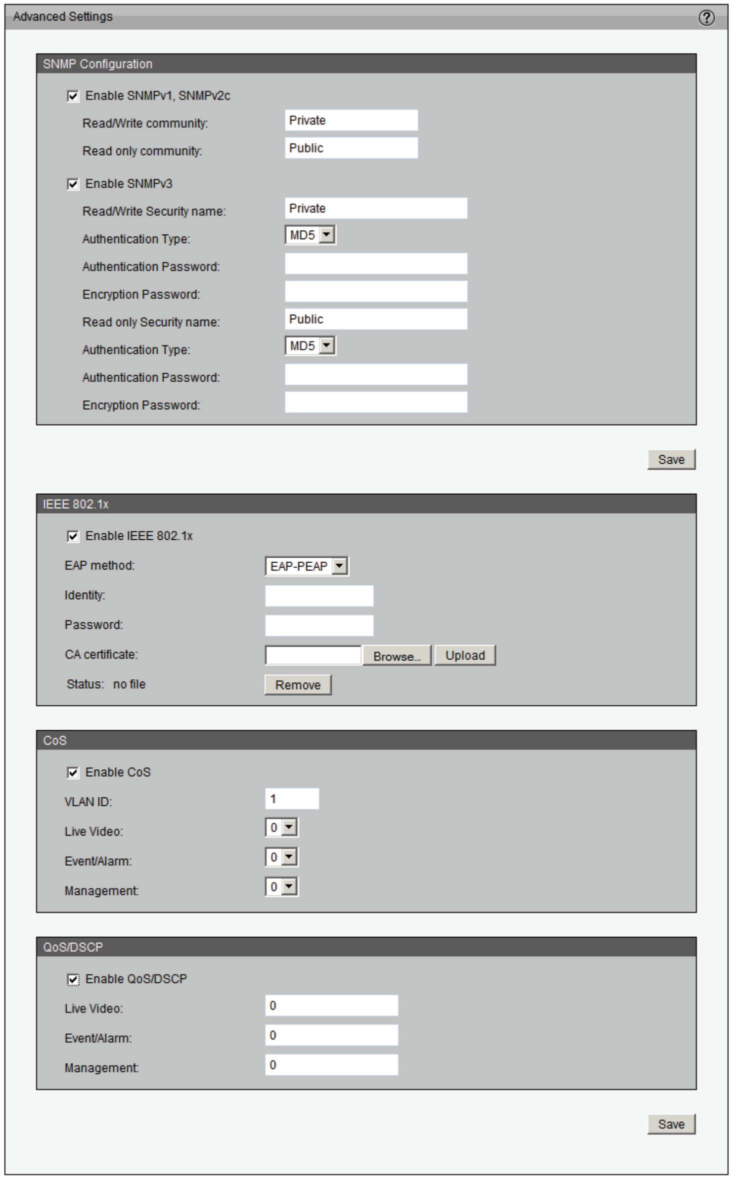
**CoS**
IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS, Class of Service. It adds a 3-bit value to the VLAN MAC header, which indicates prioritization from 0~7 (Eight different classes of service are available). The priority is set up on the network switches, which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



Advanced Settings

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:

Encryption Password:

Read only Security name: Public

Authentication Type: MD5

Authentication Password:

Encryption Password:

IEEE 802.1x

☑ Enable IEEE 802.1x

EAP method: EAP-PEAP

Identity:

Password:

CA certificate:

Status: no file

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

**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.

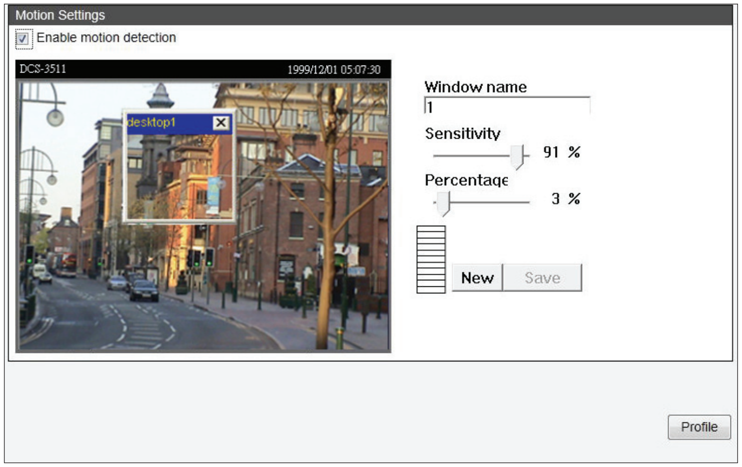
***Note:*** *Setting a higher sensitivity and a lower percentage will make motion easier to be detected.*

**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.



Motion Settings

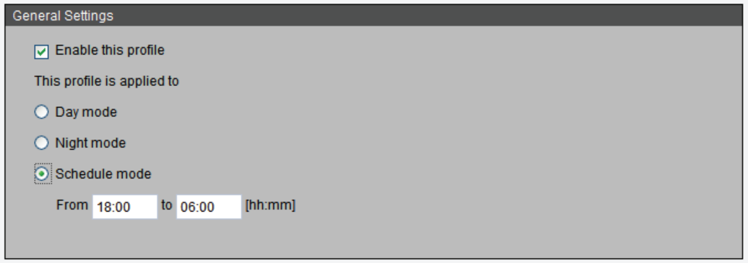
☑ Enable motion detection

DCS-3511 1999/12/01 05:07:30

Window name: 1

Sensitivity: 91 %

Percentage: 3 %



General Settings

☑ Enable this profile

This profile is applied to

○ Day mode

○ Night mode

● Schedule mode

From 18:00 to 06:00 [hh:mm]

**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.

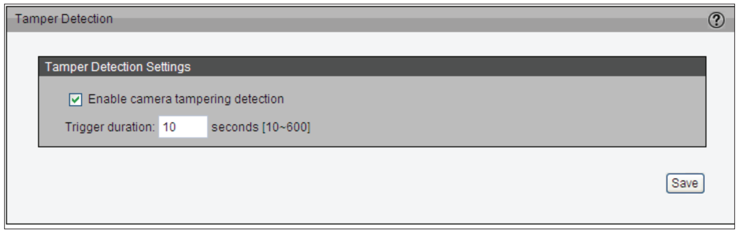
# Tamper Detection

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**. Refer to *Event Settings* for detailed information.



Tamper Detection

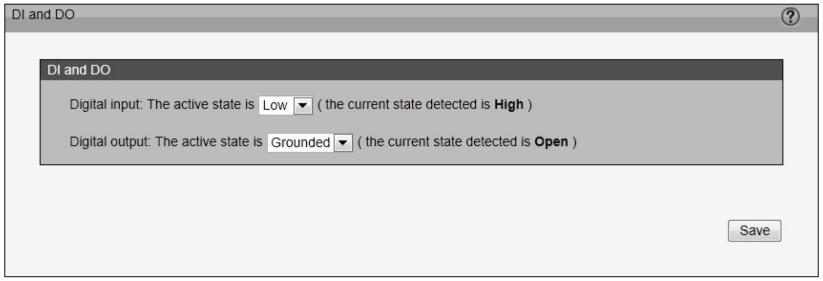
Tamper Detection Settings

☑ Enable camera tampering detection

Trigger duration: 10 seconds [10~600]

# DI and DO

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



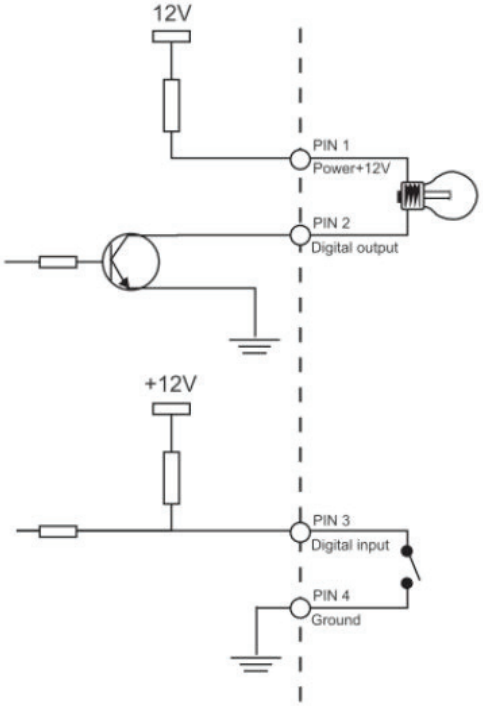
DI and DO

DI and DO

Digital input: The active state is Low ▾ ( the current state detected is **High** )

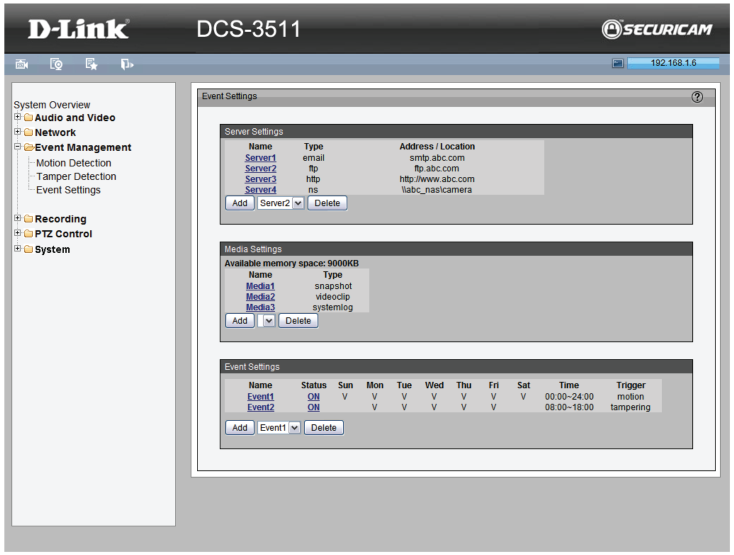
Digital output: The active state is Grounded ▾ ( the current state detected is **Open** )

## DI/DO Schematics



# Event Settings

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



Server Settings

| Name | Type | Address / Location |
|---|---|---|
| Server1 | email | smtp.abc.com |
| Server2 | ftp | ftp.abc.com |
| Server3 | http | http://www.abc.com |
| Server4 | ns | \\abc_nas\camera |

Media Settings

Available memory space: 9000KB

| Name | Type |
|---|---|
| Media1 | snapshot |
| Media2 | videoclip |
| Media3 | systemlog |

Event Settings

| Name | Status | Sun | Mon | Tue | Wed | Thu | Fri | Sat | Time | Trigger |
|---|---|---|---|---|---|---|---|---|---|---|
| Event1 | ON | V | V | V | V | V | V | V | 00:00~24:00 | motion |
| Event2 | ON |  | V | V | V | V | V |  | 08:00~18:00 | tampering |

## Sever Settings

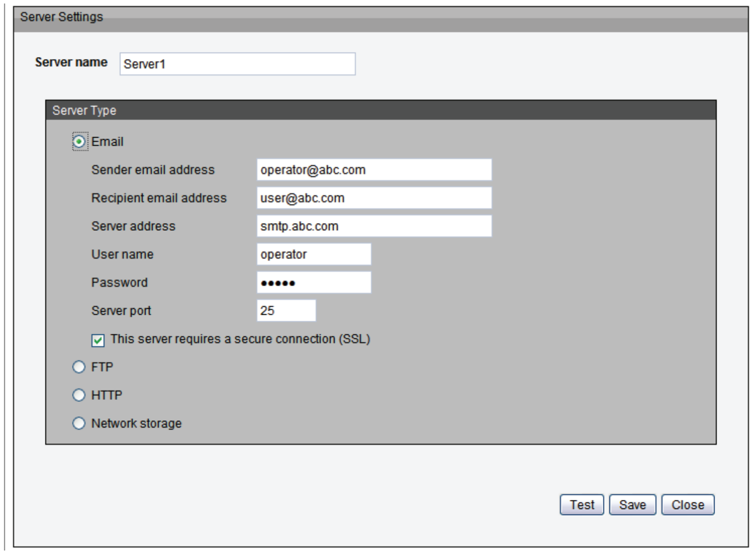
Click **Add Server** on Event Settings page to open the Server Setting page. On this page, you can specify where the notification messages are sent when a trigger is activated. A total of five server settings can be configured.

**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.



Server name: Server1

● Email

| | |
|---|---|
| Sender email address | operator@abc.com |
| Recipient email address | user@abc.com |
| Server address | smtp.abc.com |
| User name | operator |
| Password | ••••• |
| Server port | 25 |

☑ This server requires a secure connection (SSL)

○ FTP

○ HTTP

○ Network storage

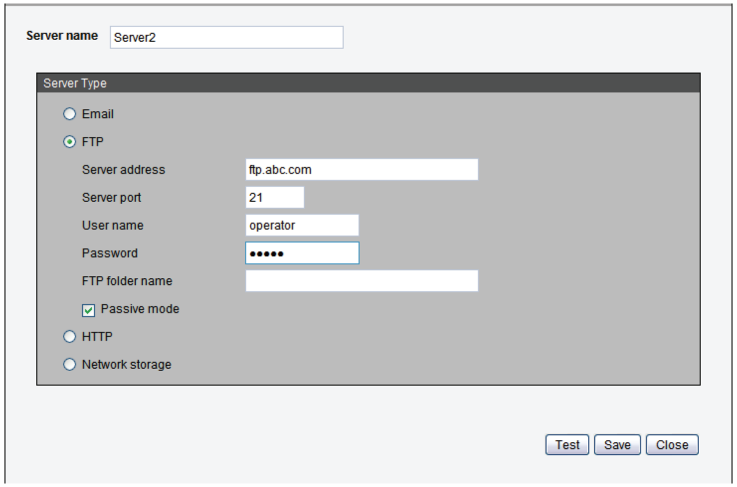
If your SMTP server requires a secure connection (SSL), select **This server requires a secure connection (SSL)**.

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.



Server name: Server2

Server Type

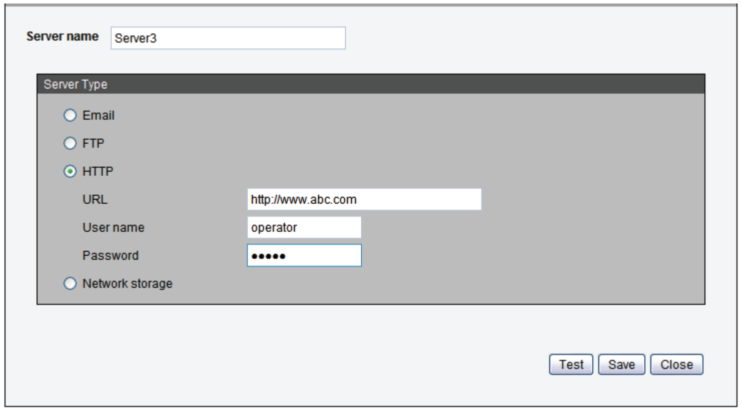
○ Email
● FTP
Server address: ftp.abc.com
Server port: 21
User name: operator
Password: •••••
FTP folder name:
☑ Passive mode
○ HTTP
○ Network storage

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.



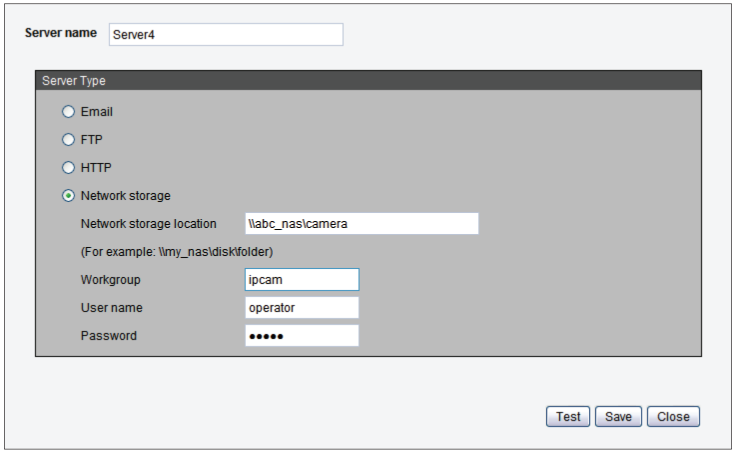
Server name: Server3

Server Type

○ Email
○ FTP
● HTTP
URL: http://www.abc.com
User name: operator
Password: •••••
○ Network storage

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 and 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.

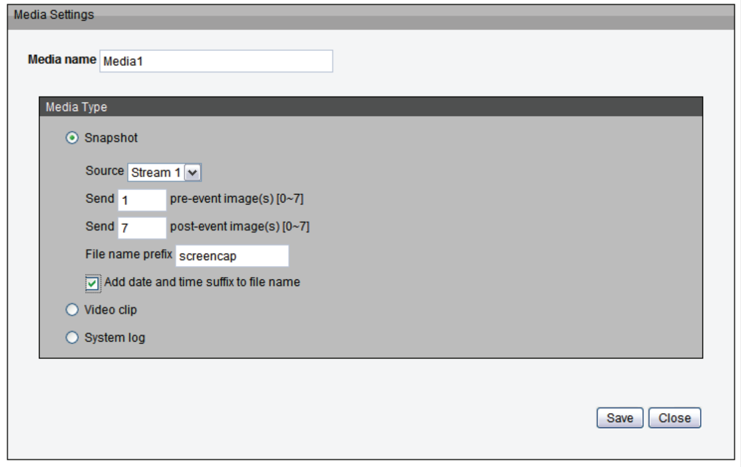


Server name: Server4

Server Type

○ Email
○ FTP
○ HTTP
● Network storage
Network storage location: \\abc_nas\camera
(For example: \\my_nas\disk\folder)
Workgroup: ipcam
User name: operator
Password: •••••

# Media Settings



Media Settings

**Media name** Media1

Media Type

● Snapshot

Source Stream 1

Send 1 pre-event image(s) [0~7]

Send 7 post-event image(s) [0~7]

File name prefix screencap

☑ Add date and time suffix to file name

○ Video clip

○ System log

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 five media settings can be configured.

**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.

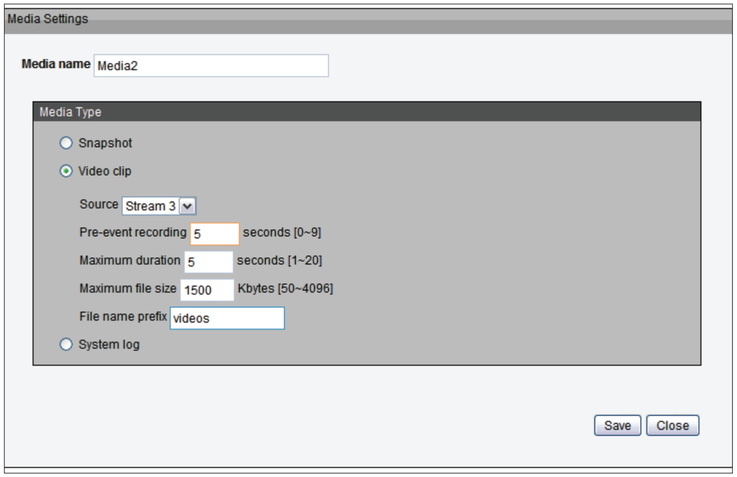
**Add date and time suffix to the file name:** Select this option to add a date/time suffix to the file name.

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



Media Settings

Media name: Media2

Media Type

○ Snapshot

● Video clip

Source: Stream 3

Pre-event recording: 5 seconds [0~9]

Maximum duration: 5 seconds [1~20]

Maximum file size: 1500 Kbytes [50~4096]

File name prefix: videos

○ System log

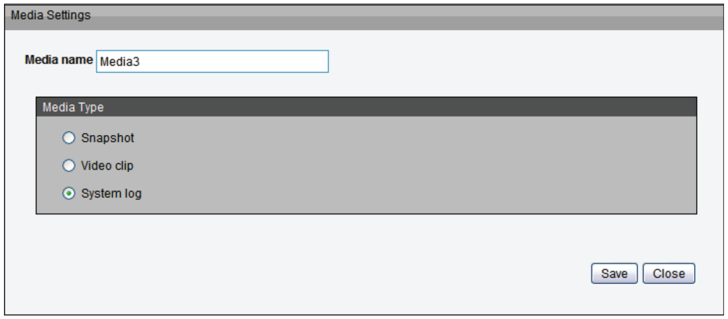
**Maximum duration:** Specify the maximum recording duration in seconds. Up to 20 seconds can be set. For example, if pre-event recording is set to 5 seconds and the maximum duration is set to 10 seconds, the camera continues to record for another 4 seconds after a trigger is activated.

**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.

**System log:** Select to send a system log when a trigger is activated.
Click **Save** to enable the settings and 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



Media Settings

Media name: Media3

Media Type

○ Snapshot

○ Video clip

● System log

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

**Event name:** Enter a name for the event.

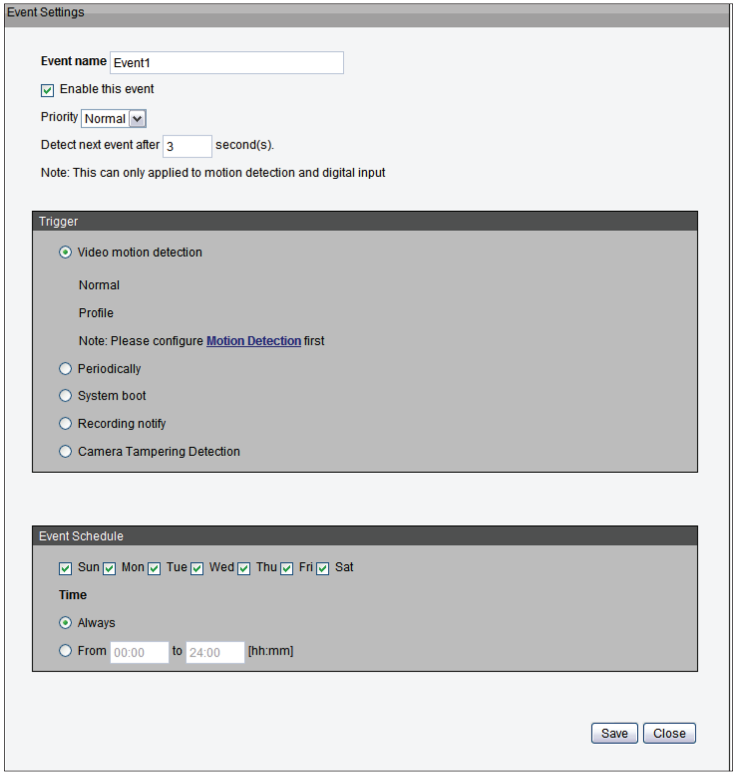
**Enable this event:** Select to activate this event.

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

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

# Trigger

This is the cause or stimulus which defines when to trigger the camera. The trigger source can be configured to use the camera's built-in motion detection mechanism. 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.


Event Settings

**Event name** Event1

☑ Enable this event

Priority Normal

Detect next event after 3 second(s).

Note: This can only applied to motion detection and digital input

Trigger

● Video motion detection

Normal

Profile

Note: Please configure Motion Detection first

○ Periodically

○ System boot

○ Recording notify

○ Camera Tampering Detection

Event Schedule

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

**Time**

● Always

○ From 00:00 to 24:00 [hh:mm]

**Video motion detection:** This option makes use of the built-in motion detection mechanism as a trigger source. To enable this function, you need to configure a Motion Detection Window first. For more information, please refer to Motion Detection 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

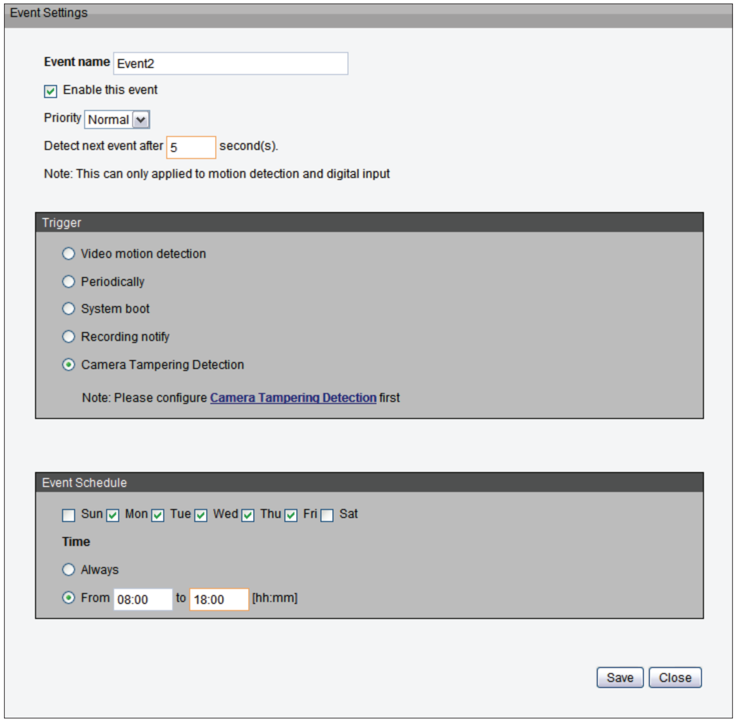
1. Select the days of the week.
2. Select the recording schedule in 24-hr time format.

### 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



Event Settings

Event name: Event2

☑ Enable this event

Priority: Normal

Detect next event after 5 second(s).

Note: This can only 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

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Time

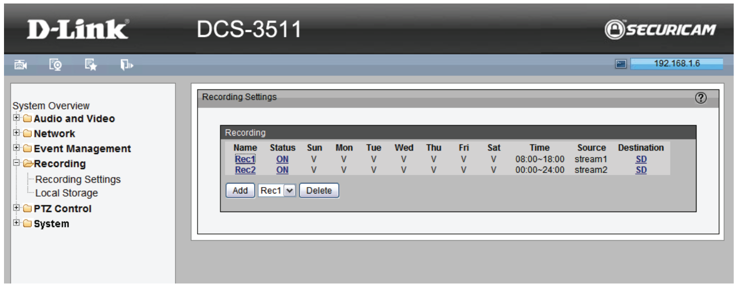
○ Always

● From 08:00 to 18:00 [hh:mm]

# 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 two recording settings can be configured.



| Name | Status | Sun | Mon | Tue | Wed | Thu | Fri | Sat | Time | Source | Destination |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Rec1 | ON | V | V | V | V | V | V | V | 08:00~18:00 | stream1 | SD |
| Rec2 | ON | V | V | V | V | V | V | V | 00:00~24:00 | stream2 | SD |

**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, or 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).

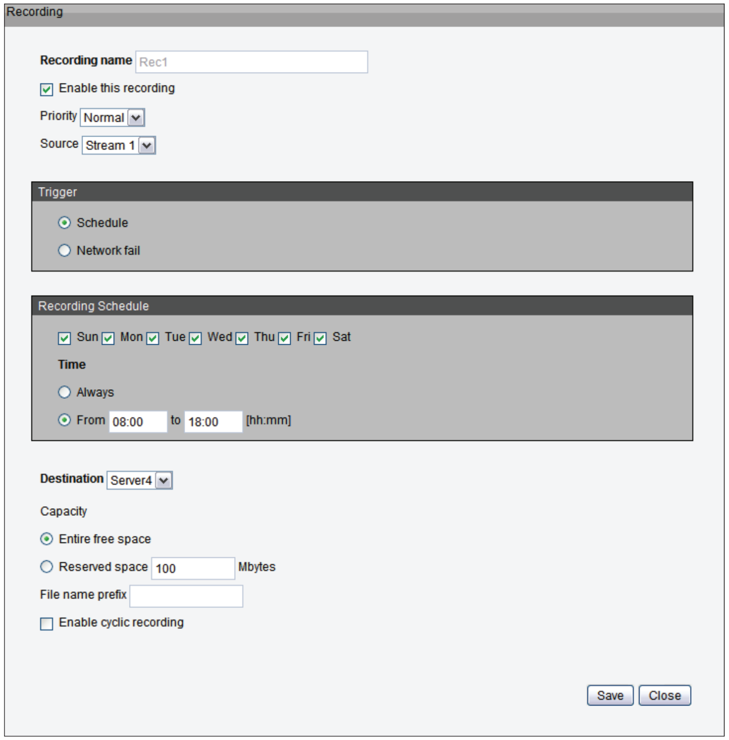
**Recording Schedule:** Specify the recording duration.

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.



Recording name Rec1

☑ Enable this recording

Priority Normal

Source Stream 1

● Schedule

○ Network fail

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Time

○ Always

● From 08:00 to 18:00 [hh:mm]

Destination Server4

Capacity

● Entire free space

○ Reserved space 100 Mbytes

File name prefix

☐ Enable cyclic recording

**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 15MB.

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.

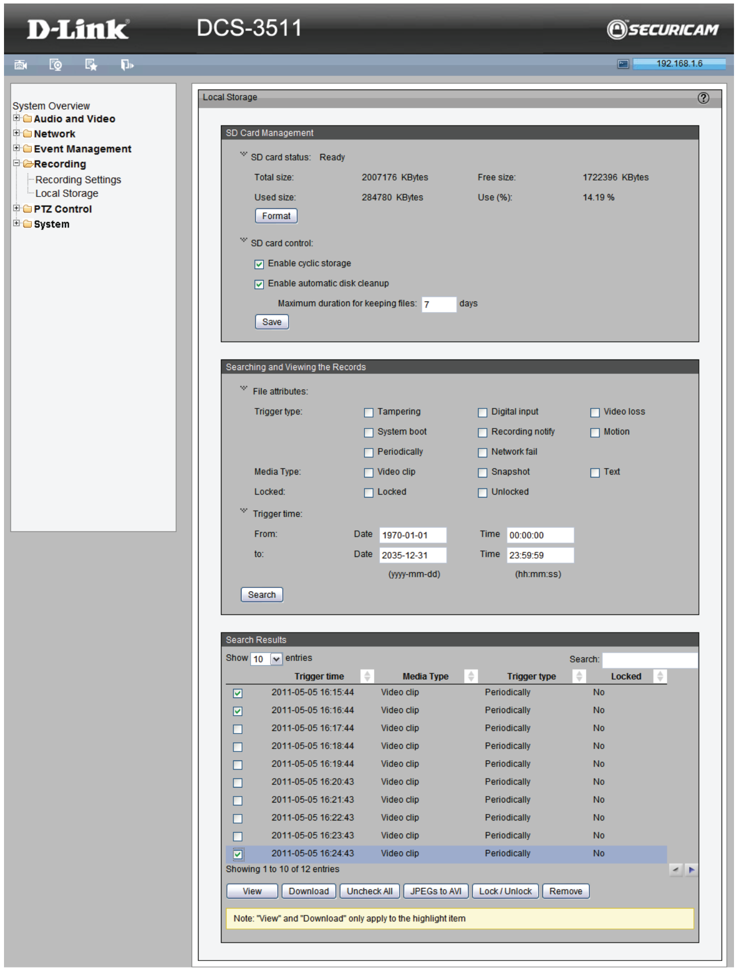
## Searching and Viewing the Records

This column allows the user to set up search criteria for recorded data. If you do not select any criteria and click the **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 the *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 the up and down arrows to sort the search results in either direction.



SD Card Management

SD card status: Ready

| | | | |
|---|---|---|---|
| Total size: | 2007176 KBytes | Free size: | 1722396 KBytes |
| Used size: | 284780 KBytes | Use (%): | 14.19 % |

SD card control:

☑ Enable cyclic storage

☑ Enable automatic disk cleanup

Maximum duration for keeping files: 7 days

Searching and Viewing the Records

File attributes:

| | | | |
|---|---|---|---|
| Trigger type: | □ Tampering | □ Digital input | □ Video loss |
| | □ System boot | □ Recording notify | □ Motion |
| | □ Periodically | □ Network fail | |
| Media Type: | □ Video clip | □ Snapshot | □ Text |
| Locked: | □ Locked | □ Unlocked | |

Trigger time:

From: Date 1970-01-01 Time 00:00:00

to: Date 2035-12-31 Time 23:59:59

(yyyy-mm-dd) (hh:mm:ss)

Search Results

Show 10 entries Search:

| | Trigger time | Media Type | Trigger type | Locked |
|---|---|---|---|---|
| ☑ | 2011-05-05 16:15:44 | Video clip | Periodically | No |
| ☑ | 2011-05-05 16:16:44 | Video clip | Periodically | No |
| □ | 2011-05-05 16:17:44 | Video clip | Periodically | No |
| □ | 2011-05-05 16:18:44 | Video clip | Periodically | No |
| □ | 2011-05-05 16:19:44 | Video clip | Periodically | No |
| □ | 2011-05-05 16:20:43 | Video clip | Periodically | No |
| □ | 2011-05-05 16:21:43 | Video clip | Periodically | No |
| □ | 2011-05-05 16:22:43 | Video clip | Periodically | No |
| □ | 2011-05-05 16:23:43 | Video clip | Periodically | No |
| ☑ | 2011-05-05 16:24:43 | Video clip | Periodically | No |

Showing 1 to 10 of 12 entries

Note: "View" and "Download" only apply to the highlight item

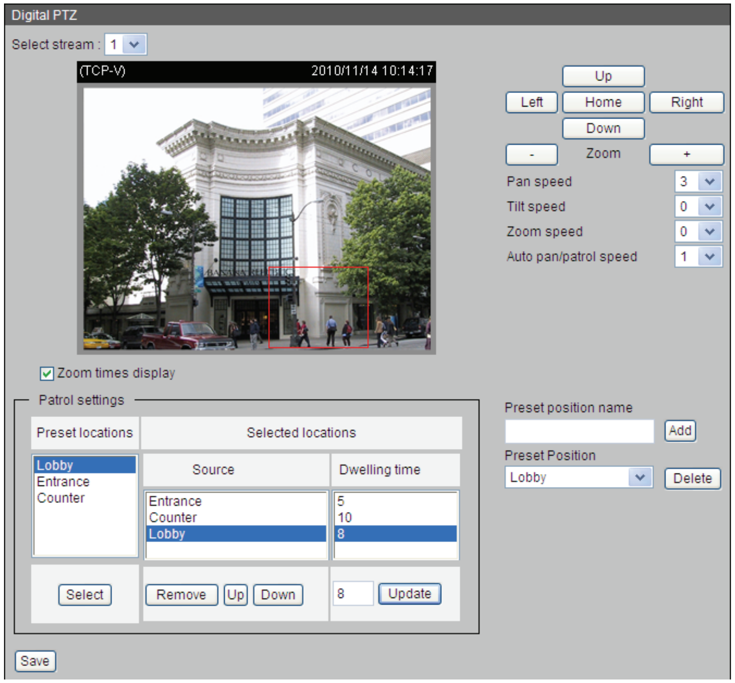
# PTZ Control

## 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, repeat steps 1 and 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.



Select stream : 1

Pan speed: 3

Tilt speed: 0

Zoom speed: 0

Auto pan/patrol speed: 1

☑ Zoom times display

Preset position name:

Preset Position: Lobby

Patrol settings

| Preset locations | Selected locations | |
|---|---|---|
| | Source | Dwelling time |
| Lobby<br>Entrance<br>Counter | Entrance<br>Counter<br>Lobby | 5<br>10<br>8 |
| | | 8 |

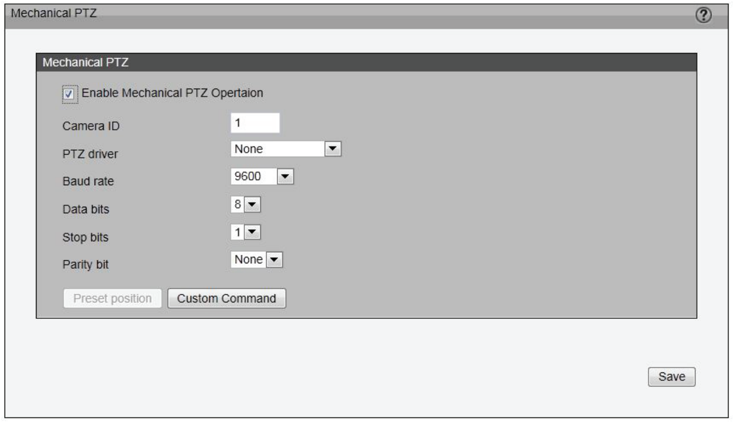
### Patrol Setting

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



Mechanical PTZ

☑ Enable Mechanical PTZ Opertaion

| | |
|---|---|
| Camera ID | 1 |
| PTZ driver | None |
| Baud rate | 9600 |
| Data bits | 8 |
| Stop bits | 1 |
| Parity bit | None |

**Enable Mechanical PTZ Operation:** Select this option to disable 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 and P protocol PTZ drivers. If your PTZ scanner does not support it, select **Custom camera (scanner)**. Please refer to the user 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.

# 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.

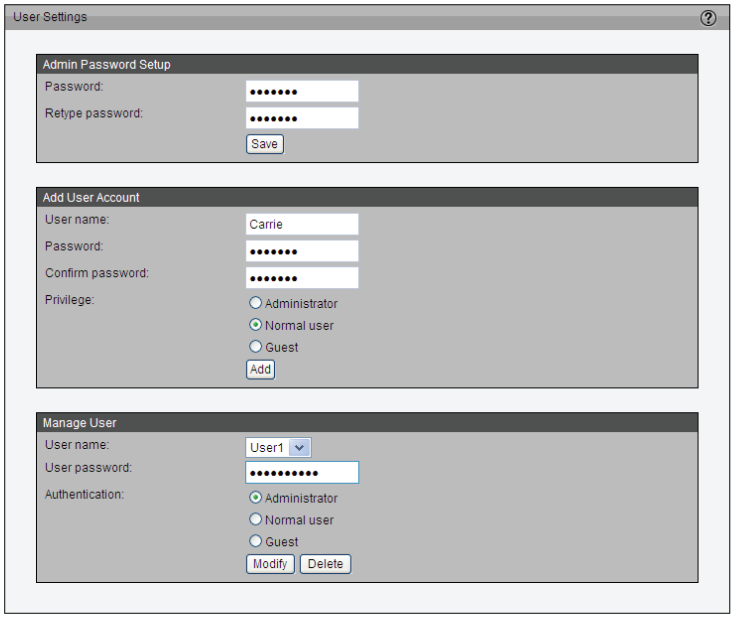
**Username:** Enter a username for the new account.

**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.



User Settings

Admin Password Setup

Password: •••••••

Retype password: •••••••

Add User Account

User name: Carrie

Password: •••••••

Confirm password: •••••••

Privilege: ○ Administrator ● Normal user ○ Guest

Manage User

User name: User1

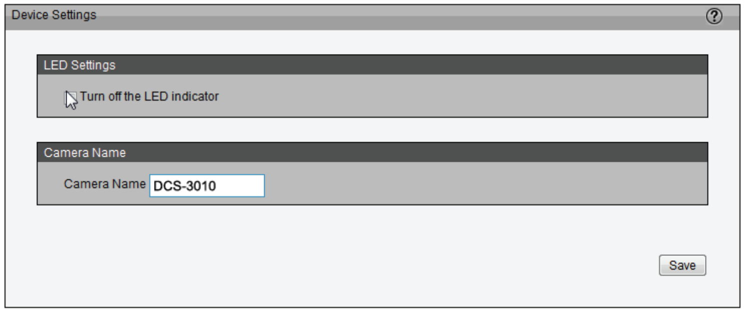
User password: •••••••••••

Authentication: ● Administrator ○ Normal user ○ Guest

# 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.



Device Settings

LED Settings

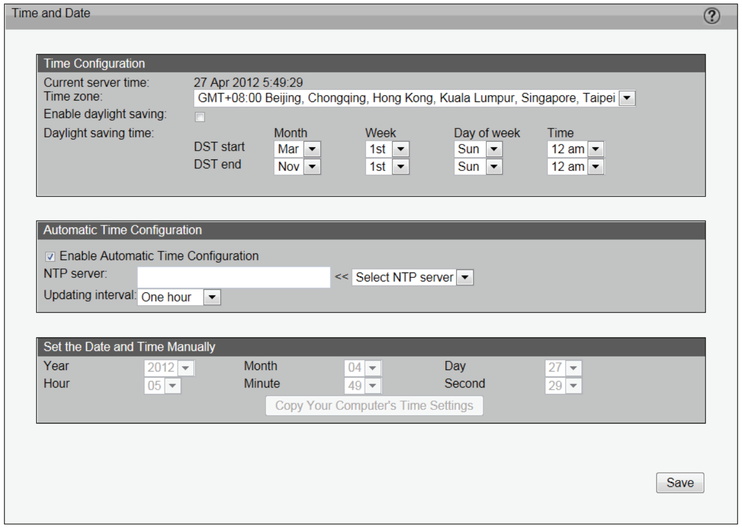
□ Turn off the LED indicator

Camera Name

Camera Name: DCS-3010

# Time and Date

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



Time and Date

Time Configuration

Current server time: 27 Apr 2012 5:49:29
Time zone: GMT+08:00 Beijing, Chongqing, Hong Kong, Kuala Lumpur, Singapore, Taipei
Enable daylight saving: □
Daylight saving time:

| | Month | Week | Day of week | Time |
|---|---|---|---|---|
| DST start | Mar | 1st | Sun | 12 am |
| DST end | Nov | 1st | Sun | 12 am |

Automatic Time Configuration

☑ Enable Automatic Time Configuration
NTP server: << Select NTP server
Updating interval: One hour

Set the Date and Time Manually

| | | | | | |
|---|---|---|---|---|---|
| Year | 2012 | Month | 04 | Day | 27 |
| Hour | 05 | Minute | 49 | Second | 29 |

**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.

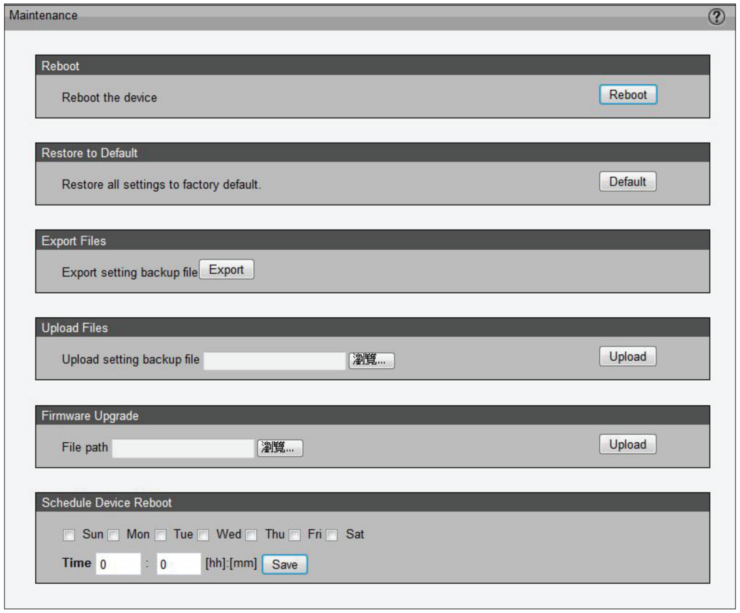
**Update Interval:** The time interval for updating the time information from NTP server.

**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.

# Maintenance

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



Maintenance

Reboot

Reboot the device [Reboot]

Restore to Default

Restore all settings to factory default. [Default]

Export Files

Export setting backup file [Export]

Upload Files

Upload setting backup file [瀏覽...] [Upload]

Firmware Upgrade

File path [瀏覽...] [Upload]

Schedule Device Reboot

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat

**Time** 0 : 0 [hh]:[mm] [Save]

**Reboot:** Click to reboot the camera. When completed, the live video page will be displayed in your browser.

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 the factory default settings.

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

**WARNING: Do not power off the camera during the upgrade!**

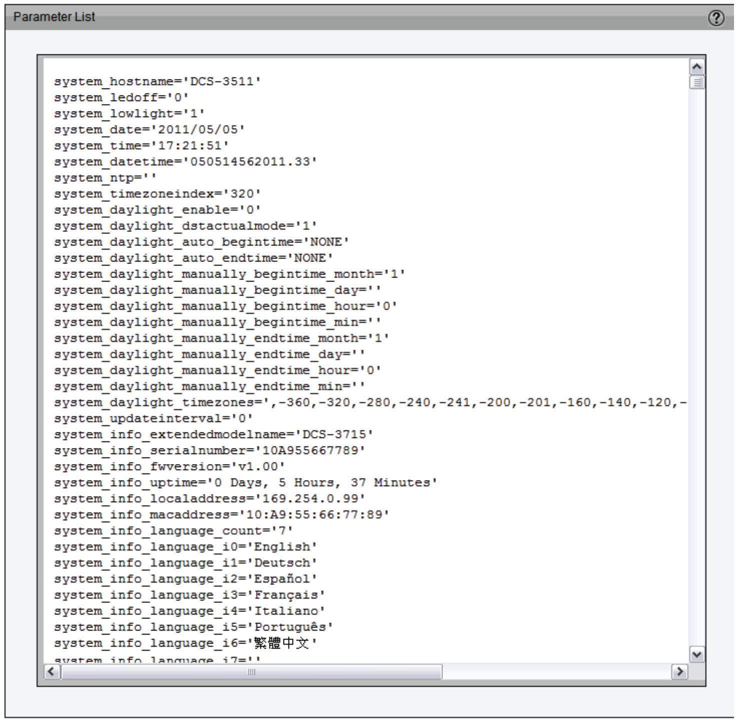
Follow the steps below to upgrade the firmware:

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

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

# Parameter List

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



```
system_hostname='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_dstactualmode='1'
system_daylight_auto_begintime='NONE'
system_daylight_auto_endtime='NONE'
system_daylight_manually_begintime_month='1'
system_daylight_manually_begintime_day=''
system_daylight_manually_begintime_hour='0'
system_daylight_manually_begintime_min=''
system_daylight_manually_endtime_month='1'
system_daylight_manually_endtime_day=''
system_daylight_manually_endtime_hour='0'
system_daylight_manually_endtime_min=''
system_daylight_timezones=',-360,-320,-280,-240,-241,-200,-201,-160,-140,-120,-
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_i0='English'
system_info_language_i1='Deutsch'
system_info_language_i2='Español'
system_info_language_i3='Français'
system_info_language_i4='Italiano'
system_info_language_i5='Português'
system_info_language_i6='繁體中文'
system_info_language_i7=''
```

# Logs

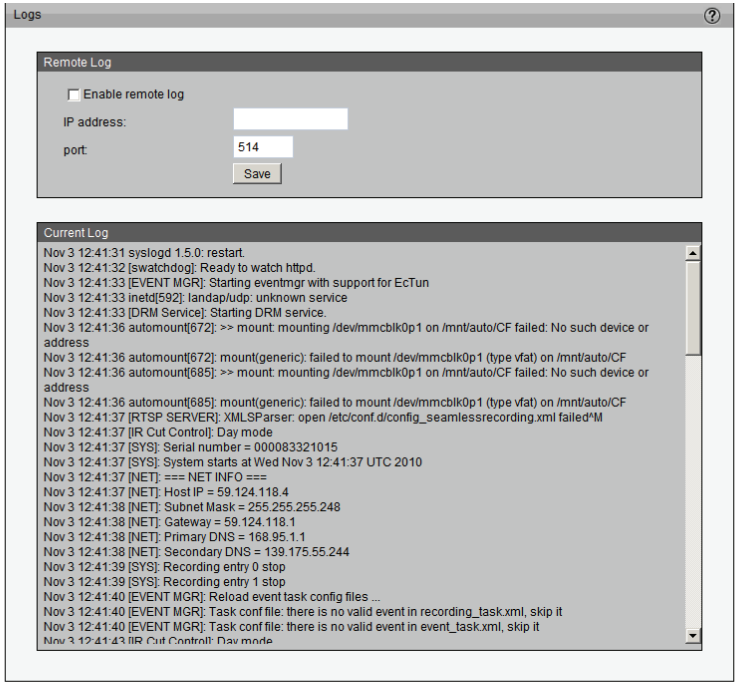
This section explains how to configure the camera to send the system log to the remote server as backup.

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

Follow the steps below to set up the remote log:

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

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



☐ Enable remote log

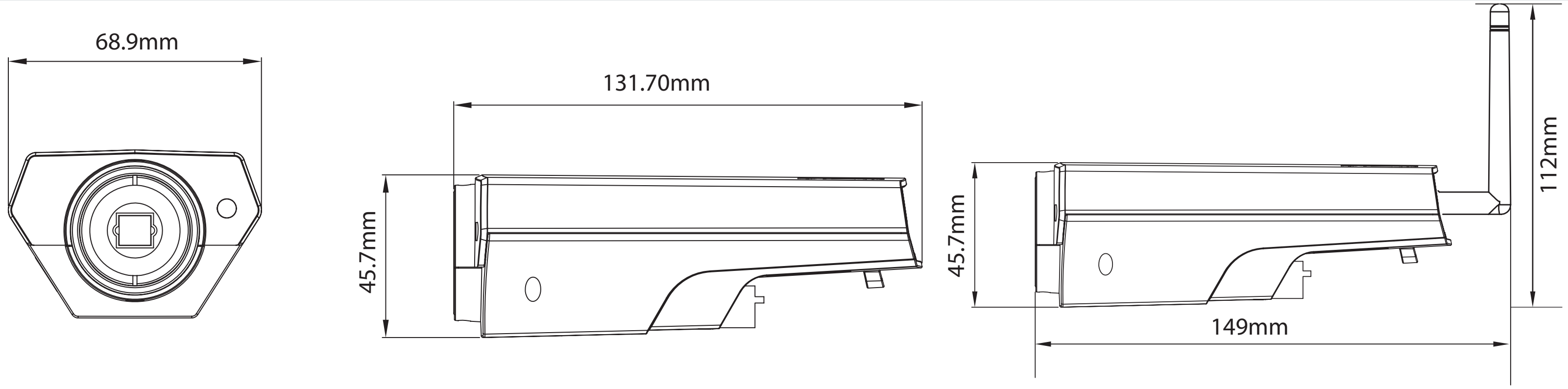
IP address:

port: 514

```
Nov 3 12:41:31 syslogd 1.5.0: restart.
Nov 3 12:41:32 [swatchdog]: Ready to watch httpd.
Nov 3 12:41:33 [EVENT MGR]: Starting eventmgr with support for EcTun
Nov 3 12:41:33 inetd[592]: landap/udp: unknown service
Nov 3 12:41:33 [DRM Service]: Starting DRM service.
Nov 3 12:41:36 automount[672]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or
address
Nov 3 12:41:36 automount[672]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF
Nov 3 12:41:36 automount[685]: >> mount: mounting /dev/mmcblk0p1 on /mnt/auto/CF failed: No such device or
address
Nov 3 12:41:36 automount[685]: mount(generic): failed to mount /dev/mmcblk0p1 (type vfat) on /mnt/auto/CF
Nov 3 12:41:37 [RTSP SERVER]: XMLSParser: open /etc/conf.d/config_seamlessrecording.xml failed^M
Nov 3 12:41:37 [IR Cut Control]: Day mode
Nov 3 12:41:37 [SYS]: Serial number = 000083321015
Nov 3 12:41:37 [SYS]: System starts at Wed Nov 3 12:41:37 UTC 2010
Nov 3 12:41:37 [NET]: === NET INFO ===
Nov 3 12:41:37 [NET]: Host IP = 59.124.118.4
Nov 3 12:41:38 [NET]: Subnet Mask = 255.255.255.248
Nov 3 12:41:38 [NET]: Gateway = 59.124.118.1
Nov 3 12:41:38 [NET]: Primary DNS = 168.95.1.1
Nov 3 12:41:38 [NET]: Secondary DNS = 139.175.55.244
Nov 3 12:41:39 [SYS]: Recording entry 0 stop
Nov 3 12:41:39 [SYS]: Recording entry 1 stop
Nov 3 12:41:40 [EVENT MGR]: Reload event task config files ...
Nov 3 12:41:40 [EVENT MGR]: Task conf file: there is no valid event in recording_task.xml, skip it
Nov 3 12:41:40 [EVENT MGR]: Task conf file: there is no valid event in event_task.xml, skip it
Nov 3 12:41:43 [IR Cut Control]: Day mode
```

# Technical Specifications

| DCS-3511/DCS-3530 | | | |
|---|---|---|---|
| Camera | Hardware Profile | ▪ 1/4” 1 Megapixel CMOS sensor<br>▪ 256 Mbytes SDRAM<br>▪ 32 Mbytes of flash memory<br>▪ 2.8~12mm fixed lens<br>▪ Shutter speed 1/5 to 1/10,000 | ▪ Aperture F1.4<br>▪ Angle of view<br>▪ 77.5~22.7° (H)<br>▪ 53.5~14.5° (V)<br>▪ 82.5~27° (D)<br>▪ Minimum Object Distance (MOD): 7.9" (0.2M) |
| | Image Features | ▪ Configurable image size, quality, frame rate, and bit rate<br>▪ Time stamp and text overlays<br>▪ 3 configurable motion detection windows | ▪ 5 configurable privacy mask zones<br>▪ Configurable brightness, saturation, contrast, and sharpness<br>▪ Min Illumination: 0.1 Lux (color), 0.05Lux (BW) |
| | Video Compression | ▪ Simultaneous H.264/MPEG-4/MJPEG format compression<br>▪ H.264/MPEG-4 multicast streaming | ▪ JPEG for still images |
| | Video Resolution | ▪ 16:9 - 1280 x 800, 1280 x 720, 640 x 360, 480 x 270, 320 x 176 up to 30 fps recording[1] | ▪ 4:3 - 1024 x 768, 800 x 600, 640 x 480, 320 x 240 up to 30 fps recording[1] |
| | Audio Features | ▪ G.711 audio encoding, bit rate: 8 kbps to 64 kbps<br>▪ MPEG-4 AAC audio encoding, bit rate: 16 kbps to 32 kbps | |
| | External Device Interfaces | ▪ 10/100 BASE-TX Fast Ethernet port<br>▪ 802.11 b/g/n wireless (for DCS-3530 only) | ▪ microSD card slot<br>▪ DIx1, DOx1<br>▪ RS485 |
| Network | Network Protocols | ▪ IPv4<br>▪ TCP/IP<br>▪ UDP<br>▪ ICMP<br>▪ DHCP client<br>▪ NTP client (D-Link)<br>▪ DNS client<br>▪ DDNS client (D-Link)<br>▪ SMTP client<br>▪ SNMP<br>▪ FTP client<br>▪ HTTP / HTTPS | ▪ Samba client<br>▪ PPPoE<br>▪ UPnP port forwarding<br>▪ RTP / RTSP/ RTCP<br>▪ IP filtering<br>▪ QoS<br>▪ CoS<br>▪ Multicast<br>▪ IGMP<br>▪ ONVIF compliant |
| | Security | ▪ Administrator and user group protection<br>▪ Password authentication<br>▪ HTTPS encryption for web brower | ▪ HTTP and RTSP digest encryption<br>▪ Remote client access control |

| | | |
|---|---|---|
| System Management | System Requirements for Web Interface | ▪ Browser: Internet Explorer, Firefox, Chrome |
| | Event Management | ▪ Motion detection<br>▪ Event notification and uploading of snapshots/video clips via e-mail or FTP<br>▪ Supports multiple SMTP and FTP servers<br>▪ Multiple event notifications<br>▪ Multiple recording methods for easy backup |
| | Remote Management | ▪ Take snapshots/video clips and save to local hard drive<br>▪ Configuration interface accessible via web browser |
| | Mobile Support | ▪ mydlink mobile app for iOS and Android mobile devices |
| | D-ViewCam™ System Requirements | ▪ Operating System: Microsoft Windows 7/Vista/XP<br>▪ Web Browser: Internet Explorer 7 or higher<br>▪ Protocol: Standard TCP/IP |
| | D-ViewCam™ Software Functions | ▪ Remote management/control of up to 32 cameras<br>▪ Viewing of up to 32 cameras on one screen<br>▪ Scheduled motion triggered, or manual recording options<br>▪ 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 | ▪ Operating: 0 to 40 °C (32 to 104 °F)<br>▪ Storage: -20 to 70 °C (-4 to 158 °F) |
| | Humidity | ▪ Operating: 20% to 80% non-condensing<br>▪ Storage: 5% to 95% non-condensing |
| | Certifications | ▪ CE<br>▪ CE LVD<br>▪ FCC<br>▪ C-Tick |
| Dimensions |  | |

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

# Contacting Technical Support

U.S. and Canadian customers can contact D-Link technical support through our web site or by phone.

Before you contact technical support, please have the following ready:

- Model number of the product (DCS-3511 or DCS-3530)
- Hardware Revision (located on the label on the bottom of the Network Camera (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the Network Camera).

You can find software updates and user documentation on the D-Link website as well as frequently asked questions and answers to technical issues.

## For customers within the United States:

**Phone Support:**
(877) 354-6555

**Internet Support:**
http://support.dlink.com

## For customers within Canada:

**Phone Support:**
(877) 354-6560

**Internet Support:**
http://support.dlink.ca

# Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. (“D-Link”) provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, or addresses with an APO or FPO.

## Limited Warranty:

D-Link warrants that the hardware portion of the D-Link product described below (“Hardware”) will be free from material defects in workmanship and materials under normal use from the date of original retail purchase of the product, for the period set forth below (“Warranty Period”), except as otherwise stated herein.

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer’s sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link’s option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement hardware need not be new or have an identical make, model or part. D-Link may, at its option, replace the defective Hardware or any part thereof with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement hardware will be warranted for the remainder of the original Warranty Period or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware or part thereof that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

## Limited Software Warranty:

D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Software Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund the portion of the actual purchase price paid that is attributable to the Software. Except as otherwise agreed by DLink in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

## Non-Applicability of Warranty:

The Limited Warranty provided hereunder for Hardware and Software portions of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

### Submitting A Claim:

The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.

- The customer must obtain a Case ID Number from D-Link Technical Support (USA 1-877-453-5465 or Canada 1-800-361-5265), who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form. Enter the assigned Case ID Number at https://rma.dlink.com/ (USA only) or https://rma.dlink.ca (Canada only).

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package o ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer and shipped to D-Link Systems, Inc.

- USA residents send to 17595 Mt. Herrmann, Fountain Valley, CA 92708. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

- Canadian residents send to D-Link Networks, Inc., 2525 Meadowvale Boulevard Mississauga, Ontario, L5N 5S2 Canada. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via Purolator Canada or any common carrier selected by D-Link. Return shipping charges shall be prepaid by D-Link if you use an address in Canada, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer. D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming. RMA phone number: 1-800-361-5265 Hours of Operation: Monday-Friday, 9:00AM – 9:00PM EST.

## What Is Not Covered:

The Limited Warranty provided herein by D-Link does not cover:

Products that, in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; and Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product.

While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited Warranty.

## Disclaimer of Other Warranties:

EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT.

IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

## Limitation of Liability:

TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NONCONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

## Governing Law:

This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This Limited Warranty provides specific legal rights and you may also have other rights which vary from state to state.

## Trademarks:

D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective owners.

### Copyright Statement:

No part of this publication or documentation accompanying this product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976 and any amendments thereto. Contents are subject to change without prior notice.

Copyright ©2013 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.

### CE Mark Warning:

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

### FCC Statement:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the
following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**FCC Caution:**

Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

If this device is going to be operated in 5.15 ~ 5.25GHz frequency range, then it is restricted in indoor environment only.

## IMPORTANT NOTICE:

**FCC Radiation Exposure Statement:**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The availability of some specific channels and/or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

**Industry Canada Notice:**

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

**IMPORTANT NOTE:**

**Radiation Exposure Statement:**

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device has been designed to operate with an antenna having a maximum gain of 2 dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

# Registration

Register your product online at registration.dlink.com

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

Version 1.0
October 15, 2013