D-Link®

Version 2.0 | 07/15/2014

User Manual

Fixed Dome Network Camera

DCS-6112/DCS-6113

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 11,2011	DCS-6112/6113 Revision A1 with firmware version 1.0
2.0	July 15, 2014	DCS-6112/6113 Revision B1 with firmware version 2.0

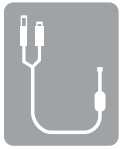
Trademarks

D-Link and the D-Link logo are trademarks or registered trademarks of D-Link. All other third-party marks mentioned herein may be trademarks of their respective owners. This publication may not be reproduced, in whole or in part, without prior express written permission from D-Link Systems, Inc.

Table of Contents

Package Contents


DCS-6112 /DCS-6113 Fixed Dome Network Camera

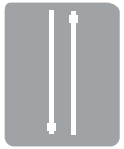

Video Out Power Cable


Power Adapter


Ethernet Cable


Security Screw Driver


Mounting Screws


Cable Tie


Alignment Sticker


User Manual and Software on CD-ROM


Quick Install Guide

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

Note: *Using a power supply with a different voltage than the one included with your camera will cause damage and void the warranty for this product.*

Minimum Requirements

- Operating System: Windows® 8, 7, or Vista® (for CD-ROM Setup Wizard)
- 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)
- Memory : At least 256MB of memory (512MB recommended)
- Web Browser: Internet Explorer® 7 or above
- VGA card resolution: SVGA or XGA (1024x768 or above)
- A 10/100 Ethernet-based network
- A microSD memory card (optional) is required for recording to onboard storage
- Broadband Internet connection (for remote access)

Introduction

The DCS-6112 and DCS-6113 indoor fixed dome network cameras are professional surveillance and security solutions for small, medium, and large enterprises. They are equipped with industry-leading high definition (Full HD) megapixel resolution. This industry-leading technology, coupled with H.264 compression, enables recording of high-quality video footage that can be viewed live over the Internet.

The DCS-6113 is capable of capturing video in both dark and light environments thanks to built-in IR LEDs and IR-cut removable (ICR) filters. The ICR filter allows the camera to capture crisp color images during the daytime and detailed gray scale images at night or in or low-light conditions.

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

Features

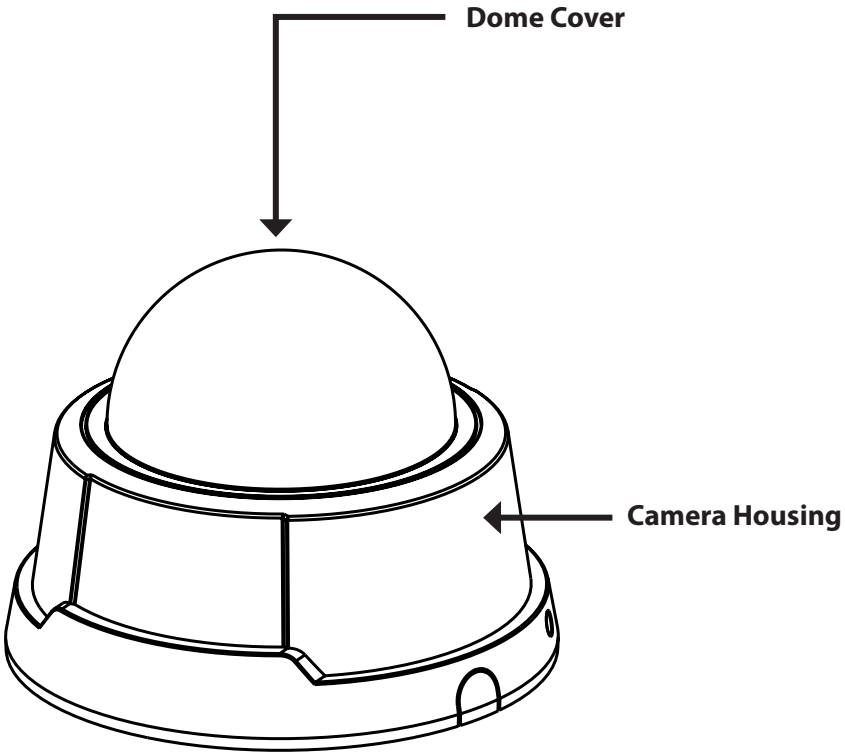
Full HD Surveillance
DCS-6112 /DCS-6113 provides Full HD industral standard 16:9 wide screen video for IP surveillance. To utilize the advantage of high resolution, the "viewing window" design can provide users flexible settings to monitor multiple ROI (Region of Interest) by a single camera. The "ePTZ" can also simulate wide area surveillance using digital zoom and pan, tilt control.

Flexible Connectivity
The DCS-6112 /DCS-6113 includes input and output ports for connectivity to external devices such as IR sensors, switches, and alarm relays. The DCS-6112 /DCS-6113 also incorporates Power over Ethernet (PoE), allowing it to be easily installed in a variety of locations without the need for supplemental power cabling.

Advanced Web User Interface
The DCS-6112 /DCS-6113 features D-Link's latest-generation graphical user interface. This freshly-designed web interface features a clean, compact, and professional home screen. Menu navigation is simplified thanks to a tree view which logically groups functions, helping users to quickly find what they need. Likewise, intuitive graphic icons reduce the amount text and clutter within the browser window. New users will appreciate the convenient contextual help which offers an easy way to find assistance with camera management tasks.

Reliable 24-Hour Surveillance
DCS-6113 is equipped with infrared LED illuminators which provide a clear picture at night for dependable 24-hour surveillance.

Hardware Overview

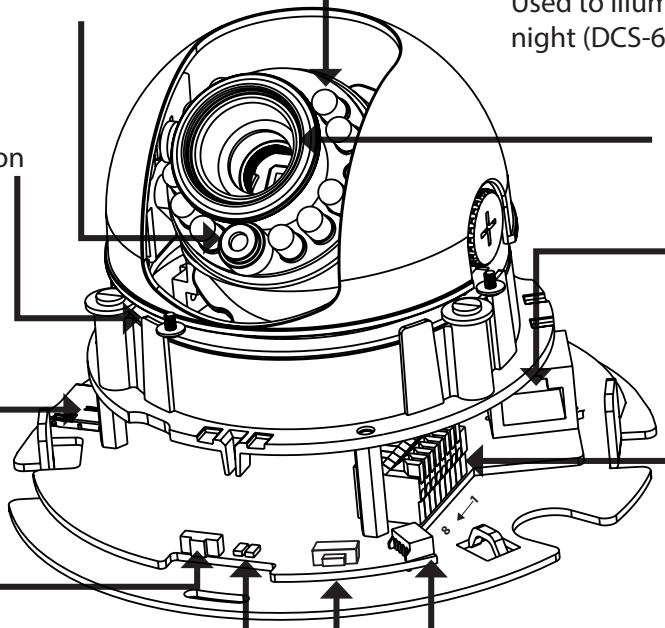


Light sensor
Judges lighting conditions and switches between day mode and night mode accordingly (Controls IR-LED and ICR on/off) (DCS-6113 only)

3-Axis Mechanism
Adjust the camera's image to achieve the desired orientation

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

Reset
Press and hold this button for 10 seconds to reset the camera



Infrared LEDs
Used to illuminate the camera's field of view at night (DCS-6113 only)

Lens
Fixed focus lens

Ethernet (PoE)
RJ-45 connector for an Ethernet cable, which can also be used to power the camera using PoE

Audio Input / Output
Audio input/output connector for an external speaker.

Digital Input (DI) /Output (DO)
DI/DO connectors provide a physical interface to send and receive digital signals to and from a variety of external devices

LED
Power and network indicator

NTSC/PAL Switch
Switch for NTSC/PAL video format

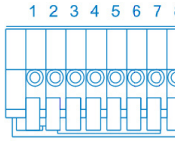
DC Input
Connects to the 12V DC power adapter to power the camera

Video Output
Video output connector for TV/Monitor

DC Input/Video Output

1. Ground of Video out
2. Video output
3. Ground of DC input
4. DC 12V

Audio I/O and DI/DO



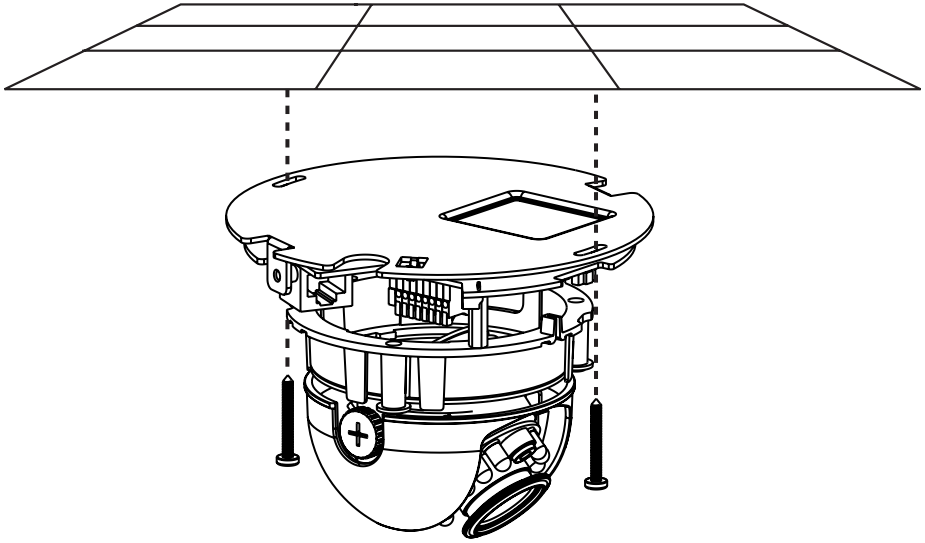
1. Audio GND
2. Audio out
3. Audio GND
4. Audio input
5. GND
6. Digital input
7. Digital output
8. 12V DC

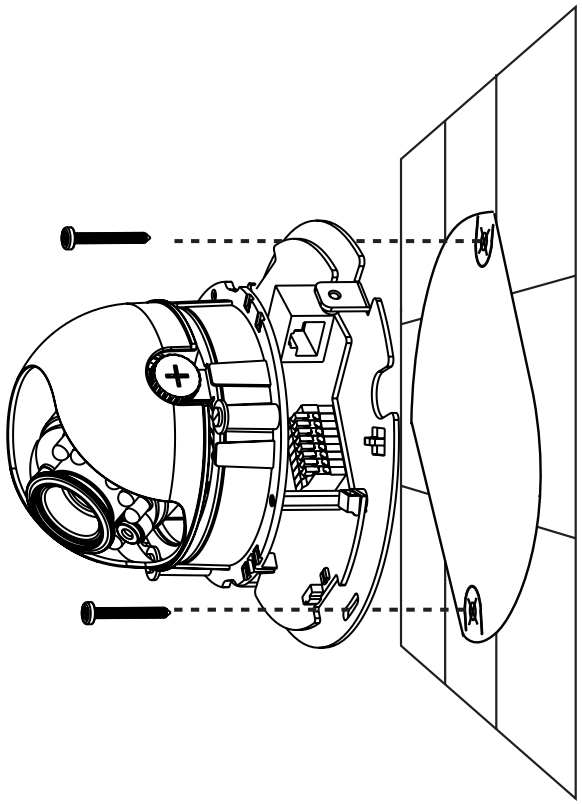
Hardware Installation

We suggest that you configure the camera before mounting it to the ceiling or wall. Refer to "Configuration with the Wizard" on page 13.

Mounting to a Ceiling or a Wall

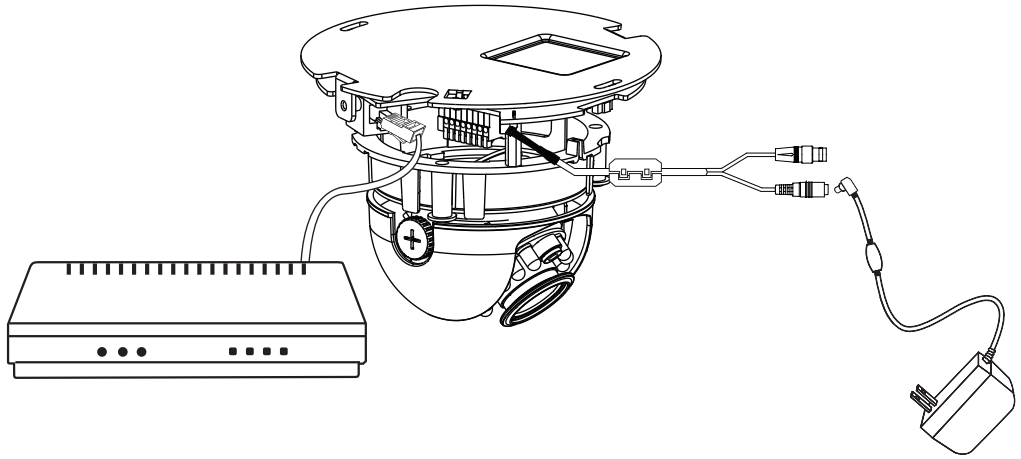
1. Locate an area on the ceiling or wall which is capable of supporting the weight of the camera.
2. Attach the alignment sticker to the ceiling or wall.
3. Drill two pilot holes where the holes of the alignment sticker are located.
4. Insert the supplied plastic anchors into the drilled holes, and align the holes at the base of the camera with the plastic anchors.
5. The camera can be mounted with the cable routed through the ceiling, wall or from the side.
6. Insert the provided screws through the holes. Use a screwdriver to tighten and secure the camera.



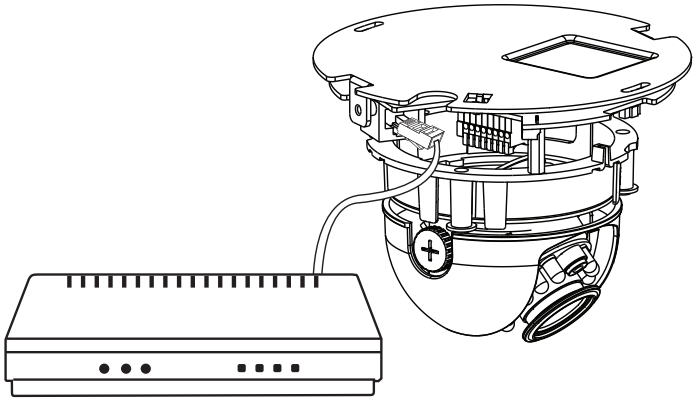


Hardware Installation

General Connection (without PoE)
Connect the network camera to a switch or router with an Ethernet cable. Then connect the supplied power cable from the camera to a power outlet.



Connection with a PoE Switch
If using a PoE switch, connect the network camera to the switch with an Ethernet cable, which will provide both power and data transmission over a single cable.

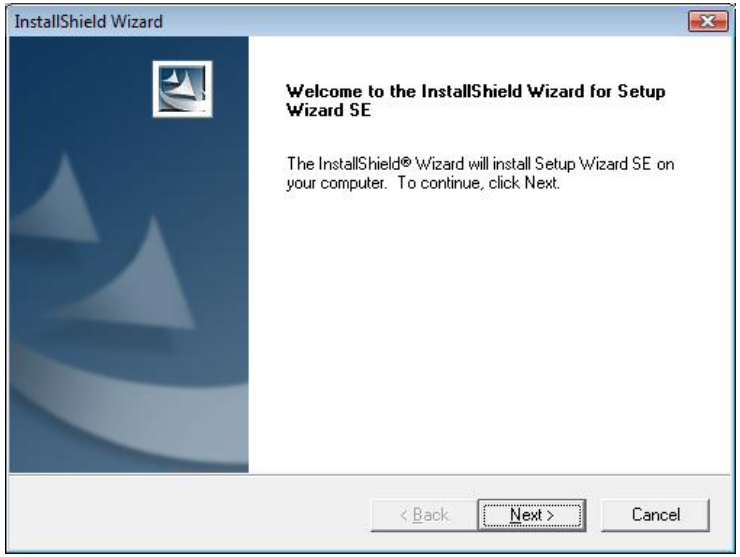


Configuration with the Wizard

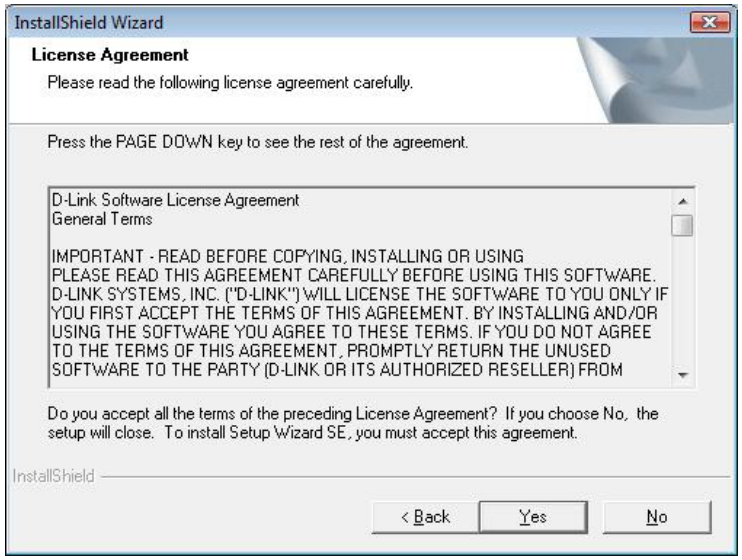
Insert the DCS-6112/DCS-6113 CD into your computer's CD-ROM drive to begin the installation. If the autorun function on your computer is disabled, or if the D-Link Launcher fails to start automatically, click **Start > Run**. Type **D:\autorun.exe**, where D: represents the drive letter of your CD-ROM drive.

Click **Setup Wizard** to begin.

The InstallShield window will open. Click **Next** to proceed with installation of the Setup Wizard.

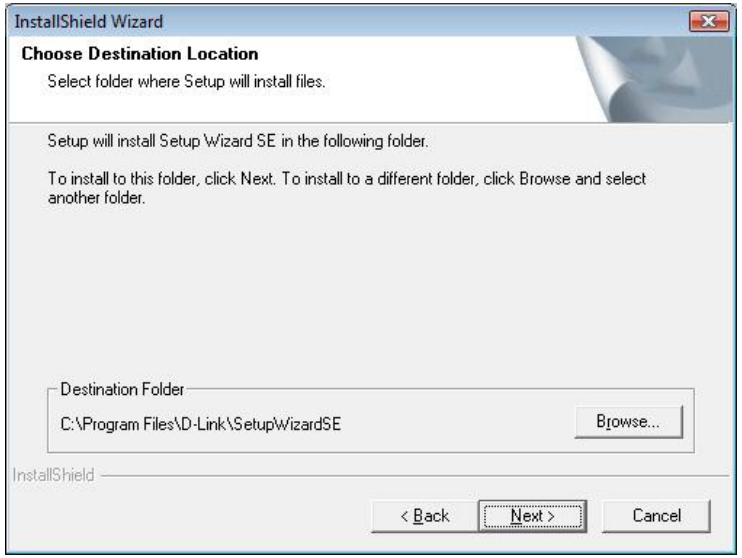


Click **Yes** to accept the terms of the License Agreement.

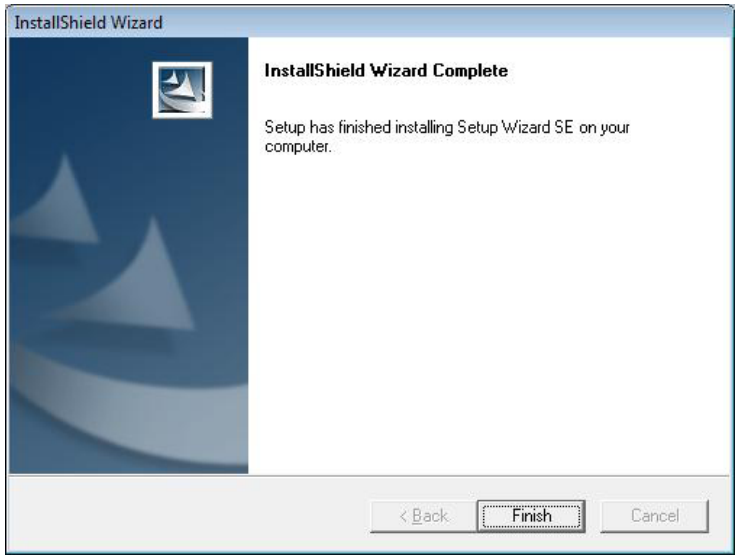


This screen will display a path to the destination folder for the installation files. Click **Browse** to select a different location, or click **Next** to proceed with installation.

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

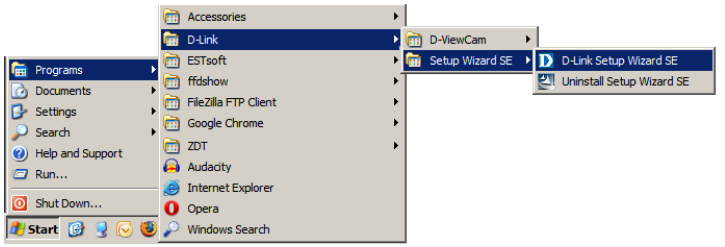


You will see this screen when the Setup Wizard has finished installing. Click **Finish** to complete the process.



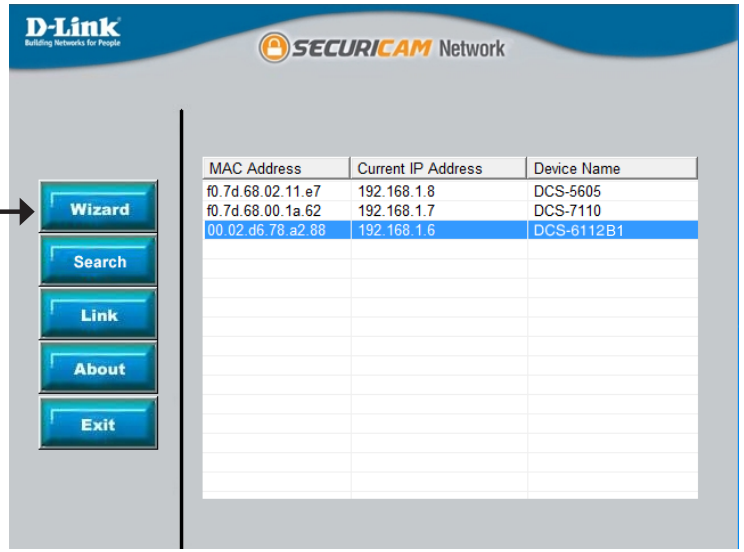
Click on the **D-Link Setup Wizard SE** icon that was created in your Windows Start menu.

Start > Programs > D-Link > Setup Wizard SE



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

Click the **Wizard** button to continue.



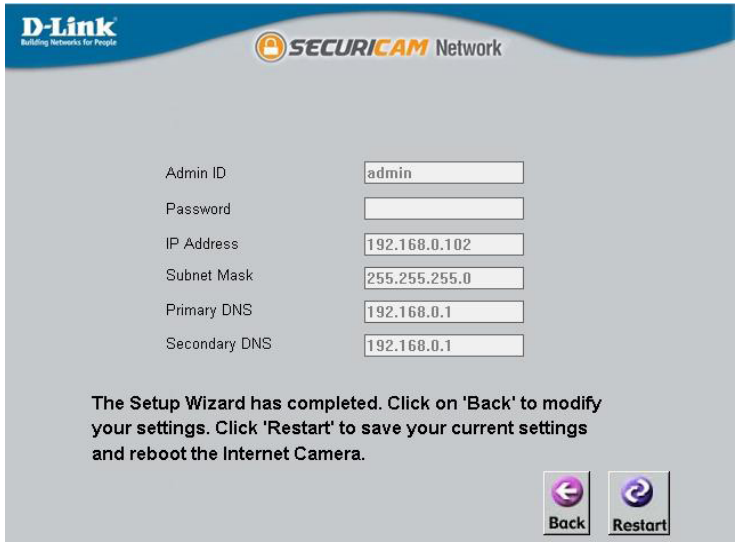
Enter the **Admin ID** and **Password**. When logging in for the first time, the default **Admin ID** is **admin** with the **Password** left blank.

Click **Next**, to proceed.

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

Click **Next**, to proceed.

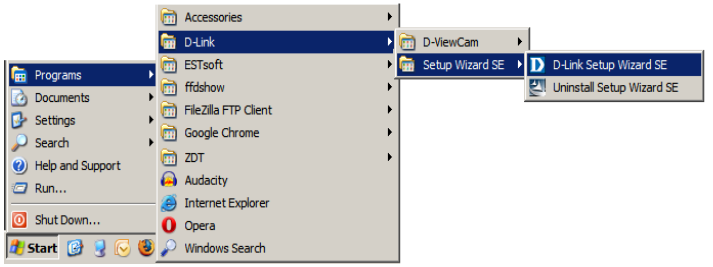
The Setup Wizard is finished. Take a moment to confirm your settings are correct. Click **Restart** to save your settings and reboot the DCS-6112/DCS-6113.



Viewing Live Video Using a Web Browser

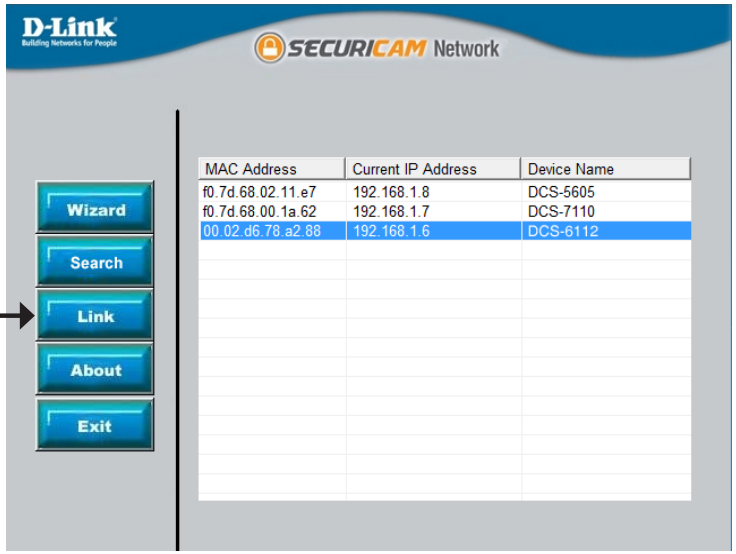
Click on the **D-Link Setup Wizard SE** icon that was created in your Windows Start menu.

Start > Programs > D-Link > Setup Wizard SE

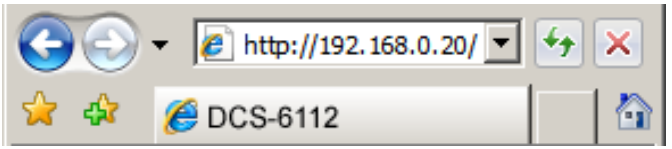


Under *Device Name*, select **DCS-6112** or **DCS-6113** and then click **Link** to access the web configuration.

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



Alternatively, you may open a web browser, such as Internet Explorer, Firefox, Safari or Chrome. Enter the default static IP address of the camera: **192.168.0.20***



***Note:** If you selected DHCP during the Setup Wizard, and your camera obtained an IP address automatically, you can get the camera's IP address from your router.*

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

View your camera's live video from this screen. You can select your video profile and operate the camera. For additional information, refer to "Live Video" on page 22.

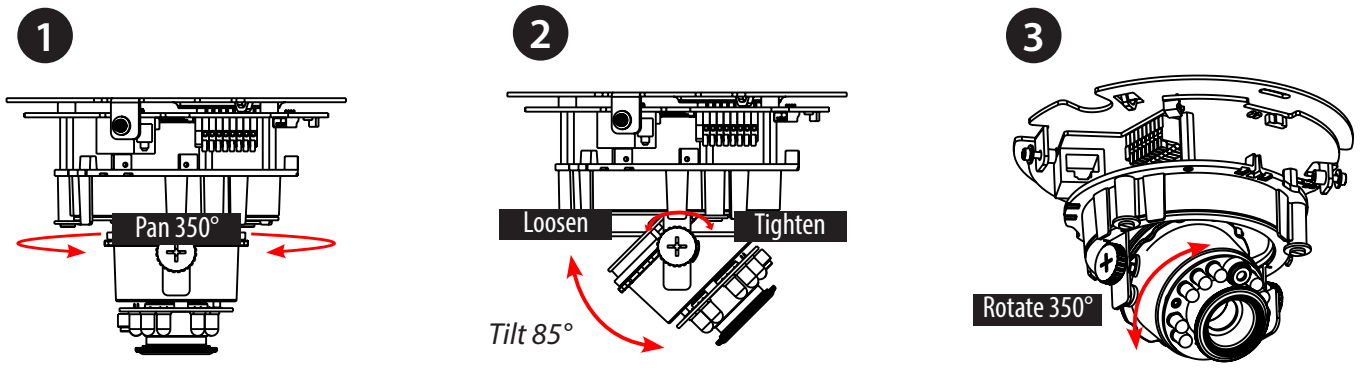
Adjust the viewing angle

Use the included security screwdriver to remove the two screws used to attach the camera housing. Slide the camera housing off, and remove the inner dome cover so you can adjust the viewing angle as described below:

1. Use a standard Phillips screwdriver to loosen the three pan screws, and turn the lens module left or right until the desired position is achieved. Tighten the pan screws once the camera is in the correct position.

2. Loosen the tilt screws on both sides of the camera and then turn the lens module up or down until the desired position is achieved. Tighten the tilt screws once the camera is in the correct position.

3. Use a small Phillips screwdriver to loosen the two screws behind the lens collar. Rotate the lens to adjust the network camera's image until the desired orientation is achieved. Tighten the screws once adjustment is completed.



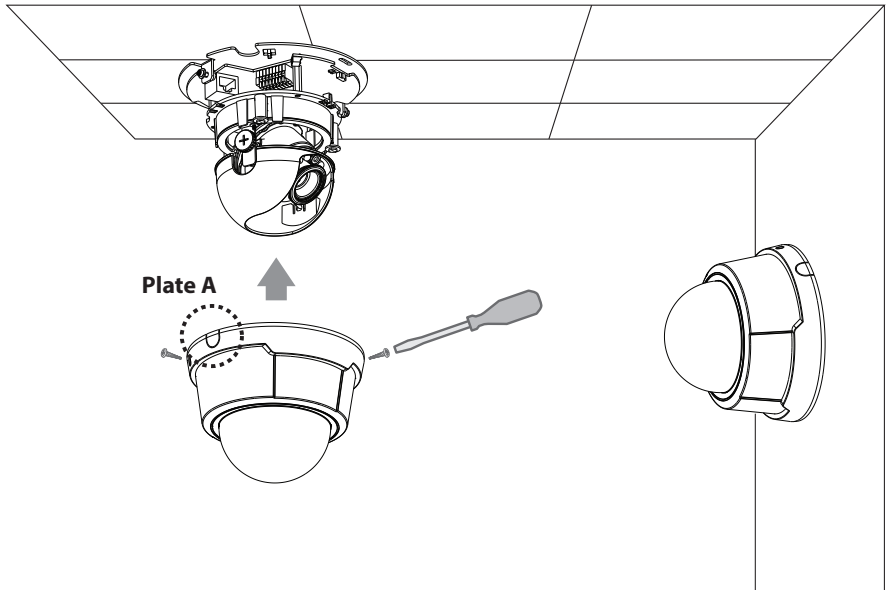
Attaching the Enclosure

1. When you slide the camera housing over the camera, align the two plastic tabs on the inside of the cover with the notches on the camera.

2. If you choose to the feed the cable through the ceiling or wall, arrange the cable neatly through the cable hole. If you choose to feed the cable from the side, remove Plate A.

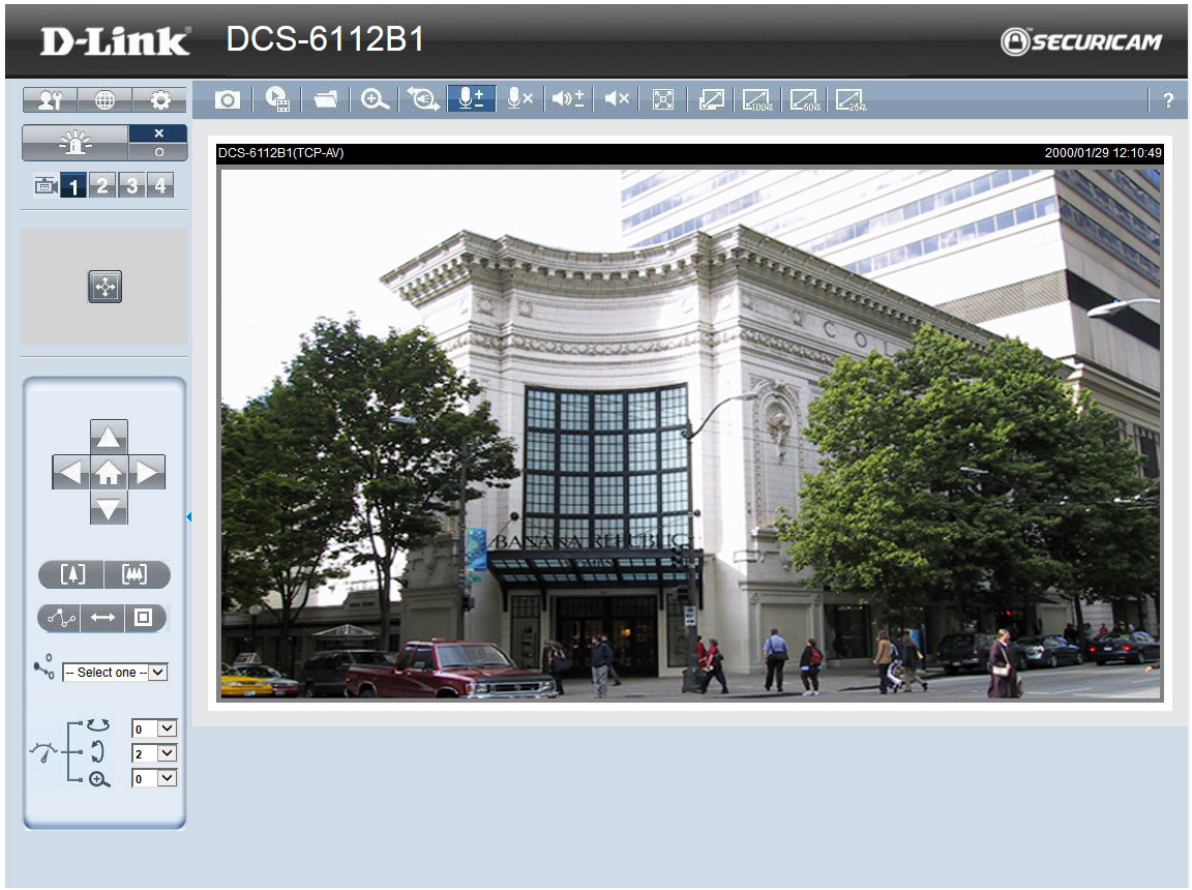
3. Attach the dome cover to the camera as the shown to the right. The dome cover cannot be attached if the angle is not correct.

4. Finally, make sure all parts of the camera are installed securely.



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 this screen. Refer to the tables on the following pages for detailed information about these icons.



D-Link Logo **Securicam Logo**	Click the D-Link logo to visit the D-Link website. The logo and website can be customized to fit your needs. For more information, refer to "User Customization" on page 64.
Client Settings	Setup the stream transmission mode and saving options on the local computer. Refer to "Client Settings" on page 26.
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. Two types of user interfaces are available: **Advanced Setup** for professional users and **Basic Setup** for entry-level users.
Digital Output	Click this button to turn the digital output device on or off.
Video Stream	This camera supports multiple streams (stream 1 ~ 4) simultaneously. You may select one for live viewing.
Global View	Click on this icon 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, refer to "Video Settings" on page 30.

ePT Direction	**Home:** Move the camera to the preset home position. **Direction:** Control the camera's pan or tilt directions (up/down/left/right).
Zoom	Zoom in/out to magnify or shrink the digital image. **Zoom in:** Magnify image **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. **Auto Pan:** Auto Pan automatically scans an area horizontally. **Stop:** Stop, Pan and Tilt.
Go Preset	**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: **Pan Speed Control** **Tilt Speed Control** **Zoom Speed Control**

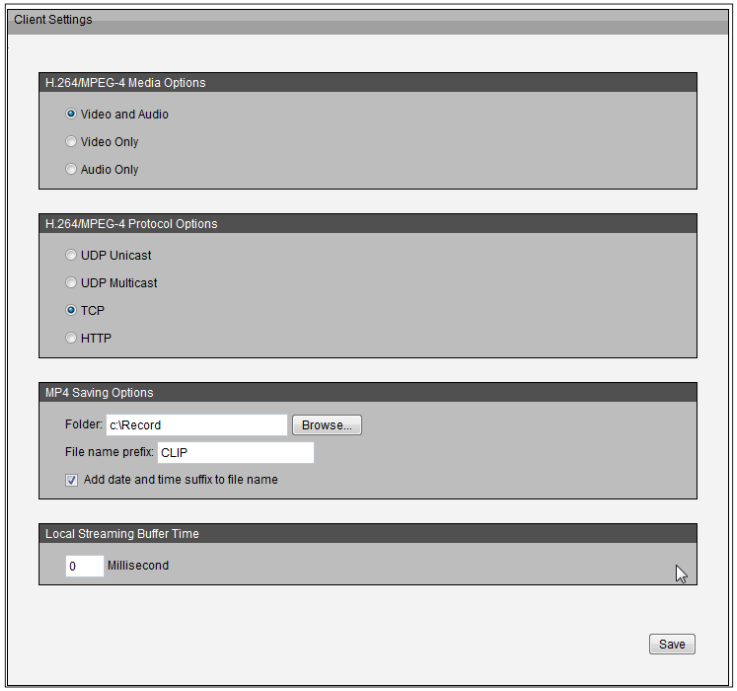
Digital PTZ Control Panel

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.
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.
Talk	Talk: If there is an external speaker connected to the camera and you have a microphone connected to your computer, you can click this button to talk to people near the camera. Press the icon again to stop talking or disable this function.
Microphone Level	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	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	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	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 on your keyboard to switch back to normal mode.
Zoom ratio	Select a **Zoom ratio:** **Auto:** The video zoom ratio will be changed automatically according to viewing window size. **100%:** Keep the video zoom ratio at 100% **50%:** Keep the video zoom ratio at 50% **25%:** Keep the video zoom ratio at 25%
Help	Click **Help** to view the detailed information regarding camera setup to help you solve any problems you encounter.

Client Settings

Click on the **Client Settings** button to configure the basic protocol options for your DCS-6112/DCS-6113.



H.264/MPEG4 Media Options
Video and Audio can be viewed at the same time, or each can be viewed separately.

H.264/MPEG4 Protocol Options
Select a protocol from the following choices:

- **UDP Unicast** - User Datagram Protocol using a one-to-one connection (streaming to a single computer)
- **UDP Multicast** - User Datagram Protocol using a one-to-many connection (streaming to multiple computers)
- **TCP** - Transmission Control Protocol, which provides higher quality video streaming than UDP. TCP includes error-checking, so it is more reliable, but not as fast as UDP.
- **HTTP** - Hypertext Transfer Protocol, which offers the highest image and video quality. However, packet loss will diminish image quality when bandwidth becomes restricted.

HTTP and UDP Considerations: If the network is protected by a firewall and it opens only HTTP port (80), HTTP protocol must be selected. In this mode, audio is disabled and only video can be viewed. UDP connections will not be available to remote users if all four ports have not been forwarded. Only the HTTP port must be forwarded for remote users to make an HTTP connection (video only). For details about ports forwarded and streaming options refer to "Port and Access Name Settings" on page 40.

MP4 Saving Options
Folder: Click on **Browse** and select the folder where you would like the MP4 file saved on your desktop computer.
File name prefix: Enter a **file name prefix** for the MP4 files.
Add date and time suffix to file name: Check the box if you would like the date and time to be added to the end of each filename.

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

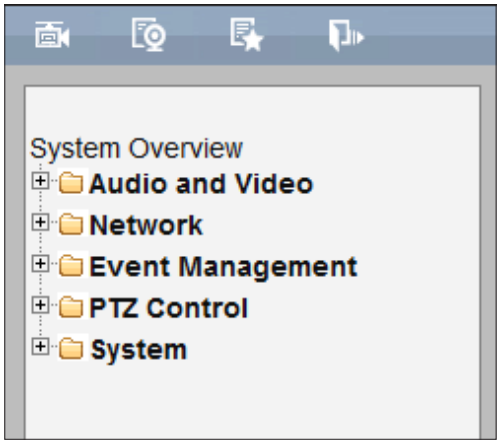
Setup

The DCS-6112 /DCS-6113 has both basic and advanced setup screens. These screens include a tree view with multiple setup options.

Basic Setup

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

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



Click the [+] next to each folder to view the options. Basic setup includes the following:

Audio and Video
- Video Settings, Audio Settings

Network
- IP Settings

Event Management
- Motion Detection, Tamper Detection

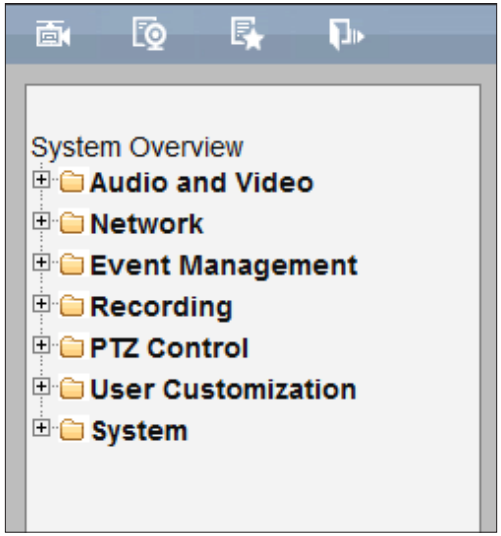
PTZ Control
- Digital PTZ (pan-tilt-zoom)

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

Advanced Setup

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

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



Click the [+] next to each folder to view the options. Advanced setup includes the following:

Audio and Video
- Video Settings, Image Settings, Audio Settings, Day and Night Settings*
  (*For DCS-6113 only)

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

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

Recording
- Recording Settings, Local Storage

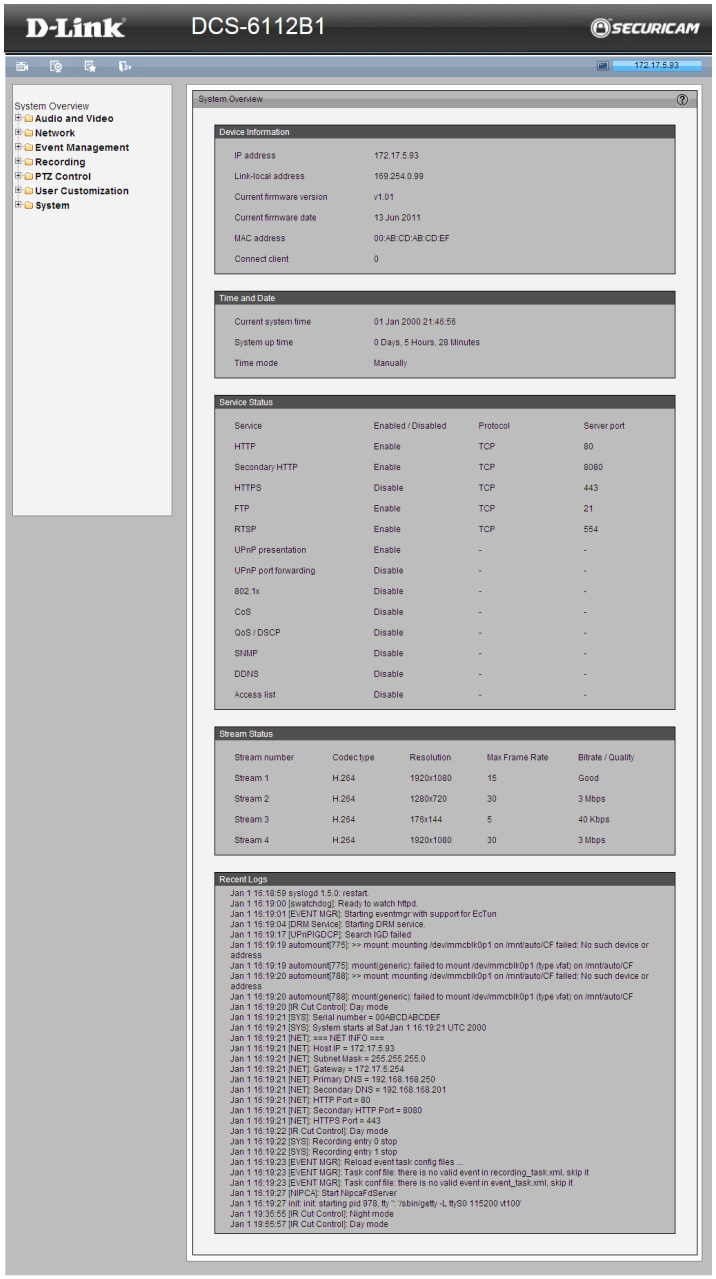
PTZ Control
- Digtal PTZ (pan-tilt-zoom)

User Customization
- Live Video Page Config, HTML Code Examples

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

System Overview

The system overview page contains a summary of the camera's current settings.



For more information about adjusting the camera's settings, refer to the following:

"Audio & Video" on page 30
"Network" on page 37
"Event Management" on page 51
"Recording" on page 60
"PTZ Control" on page 63
"User Customization" on page 64
"System" on page 66

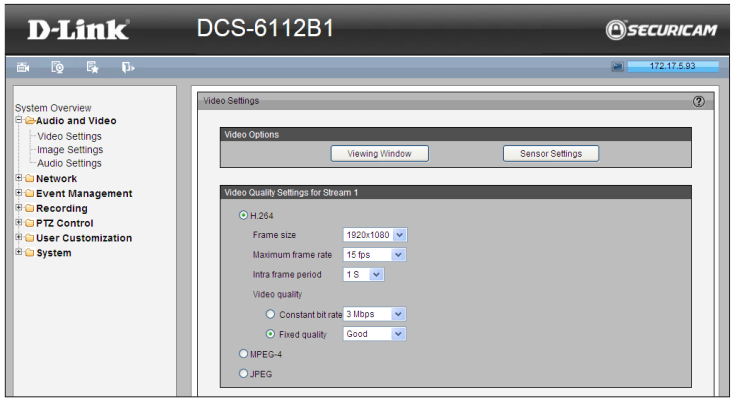
Audio & Video

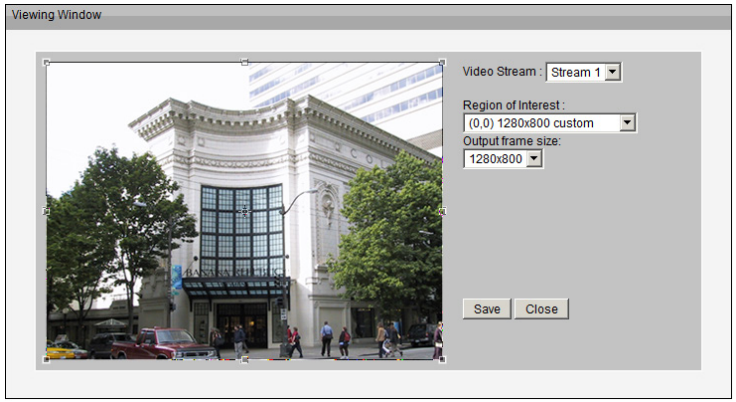
Video Settings

The Video Settings page allows you to set up multiple video streams, which can be displayed on a computer, mobile device, or storage system. Each stream has Video Quality Settings, which are independent options for compression type, frame size, and frame rate, allowing the user to reduce bandwidth while optimizing viewing quality. (Refer to "Video Quality Settings for Streams 1~4" on page 32.)

Video Options

Click **Viewing Window** to open the viewing region settings page. On this page, you can set the **Region of Interest** (ROI) and the **Output Frame Size** for multiple streams*.





Follow these steps to set up a stream:

1. Select a **Video Stream** whose viewing region you would like to set.
2. Select a **Region of Interest** from the drop-down menu. 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.
4. Click **Save** to save your settings, and click **Close** to close the window.

Note: *Make sure the* ***Output Frame Size*** *is not be greater than the* ***Region of Interest*** *(current maximum resolution).*

*You can set **Video Options** for multiple streams as follows:

Streams 1-3: Users can define the **Region of Interest** (viewing region) and the **Output Frame Size** (size of the live view window).

Stream 4: This is a global view stream that captures the full view of the video. Users can define the **Output Frame Size** (size of the live view window).

Click **Sensor Settings** to open the Sensor Settings page. You can set the **Maximum exposure time**, **Exposure level**, and **Max Gain** (Auto Gain Control) setting.

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 second.
- **Exposure level:** You can manually set the Exposure level which ranges from 1 to 8 (dark to bright).
- **Max. Gain (Auto Gain Control):** You can manually set the AGC level (2X 4X, or 8X). The higher the value, the brighter the image will be.
- **Enable BLC (Back Light Compensation):** Enable this option when the object is too dark or too bright to recognize. It allows the camera to adjust to the best light conditions in any environment and automatically give the necessary light compensation.

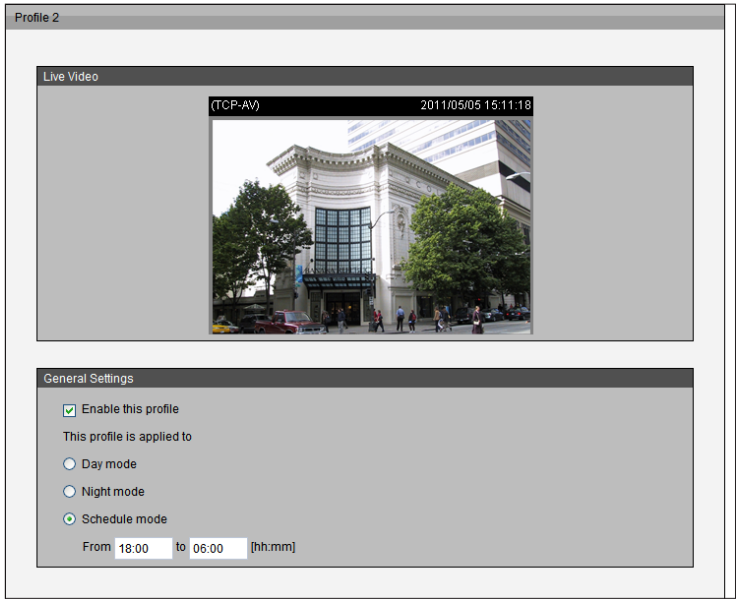
You can create two sets of sensor settings:
For example, you could use *Profile 1* for normal situations, and create a *Profile 2* for special situations that may require **Schedule mode** or **Night mode***.

* Night mode applies to the DCS-6113 only.

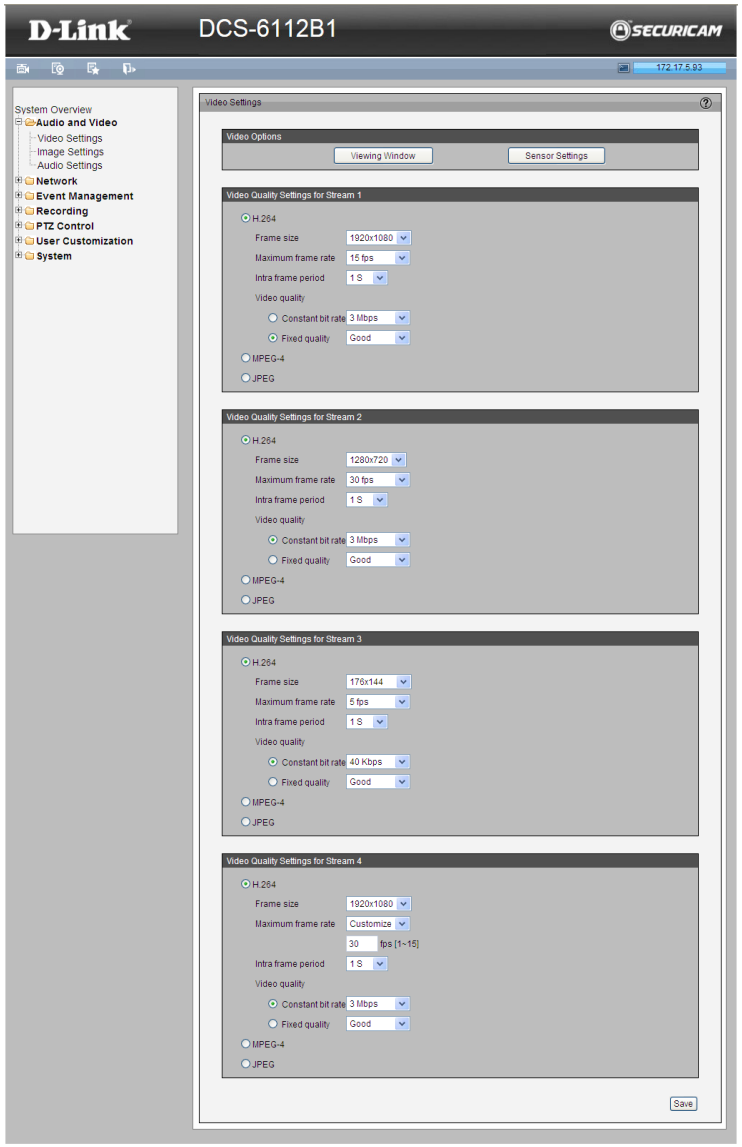
You can click **Preview** and fine-tune the image. Click **Restore** to go back to the original settings without incorporating any changes. Click **Save** to save your settings, and click **Close** to exit the page.

To configure another sensor setting, click **Profile 2** and follow the steps below:

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



Video Quality Settings for Streams 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 MPEG-4 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 12 options you can select: 320x176, 320x240, 480x270, 640x360, 640x480, 800x450, 800x600, 1024x768, 1280x720, 1280x960, 1440x1080, 1920x1080, if there is no viewing window applied. (320x176 for mobile phone. 1280x720 or 1920 x 1080 for HD display.)

Maximum Frame Rate: This option affects the smoothness of the video. Select a higher frame rate for smoother video quality, but it requires more storage. Ten options to select from: 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: The shorter the duration of the **Intra Frame Period**, 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 40 Kbps to 6 Mbps. You can also select **Customize** and manually enter a value.
- **Fixed quality:** The video quality can be adjusted by selecting one of the following: **Medium**, **Standard**, **Good**, **Detailed** and **Excellent**. You can also select **Customize** and manually enter a value.

Image Settings

The Image Settings page allows you to control the display of the video. Adjust white balance, brightness, saturation, contrast, and sharpness settings.

Color: Select either **Color** or **B/W** (black and white) for the video display.

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

Video Orientation: Select **Flip** to vertically rotate the video. Select **Mirror** to horizontally rotate the video. You may select both options if the 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 set the white balance:

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 settings.

Image Settings for Profiles

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 stamp on the video streams. (When the frame size is set to 176 x 144 only the time will be stamped on the video streams.)

Note: *The "Sensor Settings" and "Image Settings" share the same Profile 2* settings*.

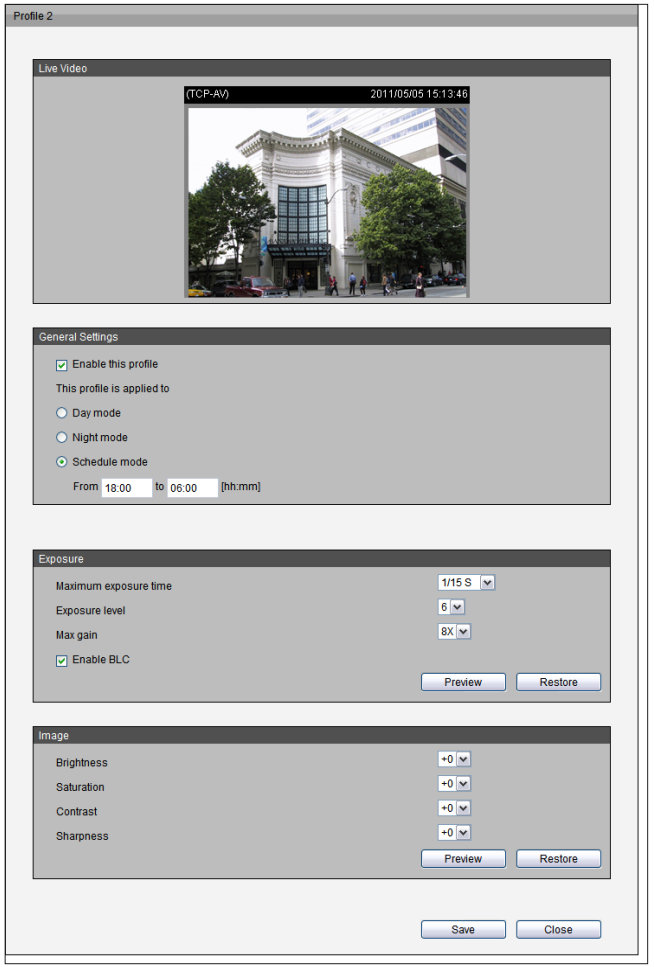
*Applies to DCS-6113 only.

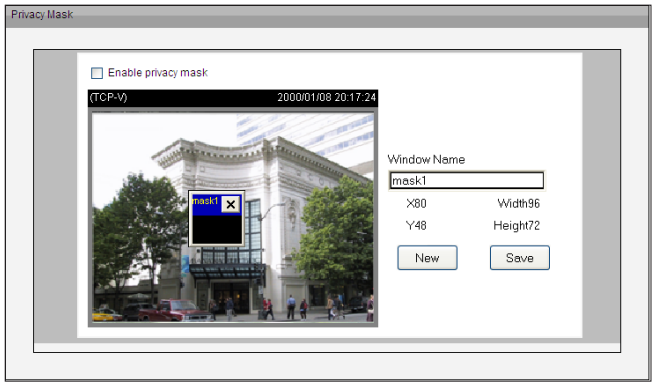
Privacy Mask: You can block out certain sensitive zones for privacy. To set up a Privacy Mask Window, follow the steps below:

1. Click **New** to create a Privacy Mask Window.
2. The height and width of the window can be resized using drag-and-drop.
3. Enter a descriptive **Window Name** and click **Save** to save changes.
4. Check the box to **Enable privacy mask**.

Notes:

- *Up to five privacy mask windows can be set up on the same screen.*
- *To delete the privacy mask window, click the X at the upper right-hand corner of the window.*





Audio Settings

Mute: Check the box to mute audio.

Note: *If the switch on the Control board is switched off (disabled audio) then this option will be disabled.*

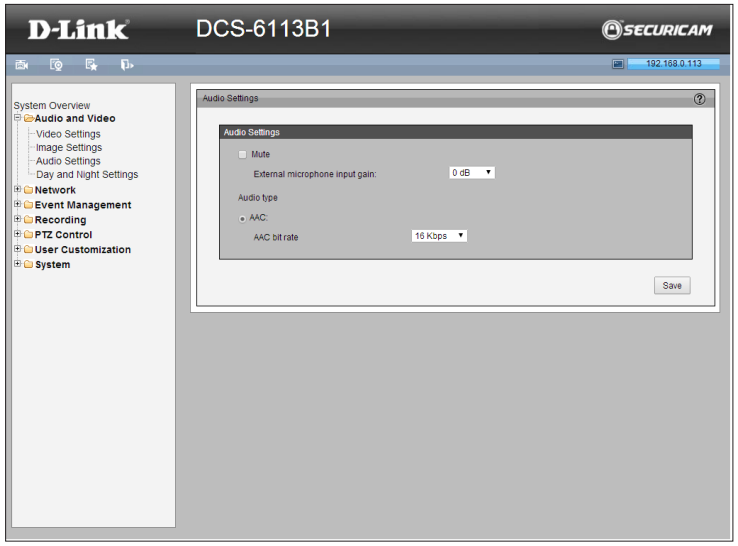
External microphone input gain: Select an external microphone input gain from the drop-down list. Set the microphone input gain at **-33dB**, **0dB**, or **21dB**.

Note: *The higher the decibel number, the louder the sound.*

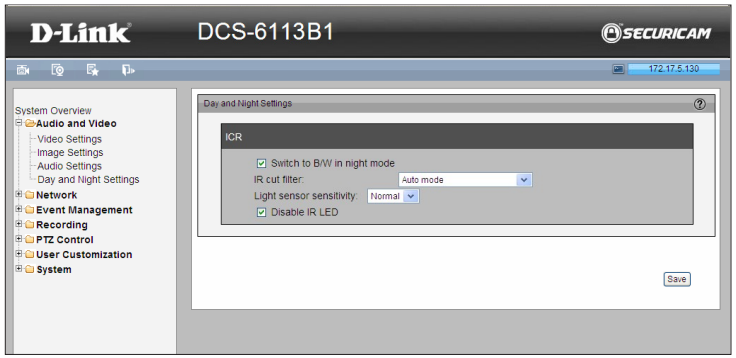
Audio type: Select Advanced Audio Coding (AAC), which is a wide band audio coding algorithm that exploits two primary coding strategies to dramatically reduce the amount of data needed to convey high-quality digital audio.

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

G.711: Select between **uLAW (G.711)** and **ALAW (G.711)** compression formats. A higher audio quality will require more bandwidth.



Day and Night Settings*



Switch to B/W in Night Mode: Check the box to automatically enable the DCS-6113 to **Switch to B/W in night mode**.

IR Cut Filter: The IR-Cut Removable (ICR) filter mechanically switches between two different sensor filters. It provides the best light conditions both during the day and night. Select an option from the drop-down menu.

The options are:

- **Auto Mode:** The camera automatically switches between day and night mode by measuring 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 DCS-6113 will switch between day and night mode based on a specific schedule. Make sure you enter the starting and ending time for the day mode. Note that the time format is [hh:mm] and is expressed in 24-hour clock time. By default, the starting time and ending time of day mode are set to 07:00 and 18:00.

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

Disable IR LED: Check the box if you want to disable the IR LED. By default, the IR LED automatically switches on at night.

* Day & Night function is for DCS-6113 only.

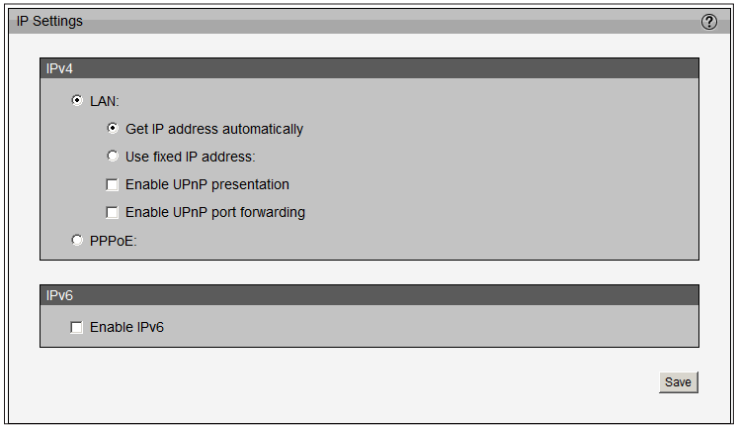
Network

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*. (If you select PPPoE, skip to the instructions on the next page.)

- **Get IP address automatically (DHCP):** Select this option if you have a DHCP server running on your network and would like a dynamic IP address to be assigned to the camera automatically.
- **Use fixed IP address:** Select this option if you want a static or fixed IP address for your camera. Then complete the fields listed below:



IP Address: Enter an **IP address**.

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

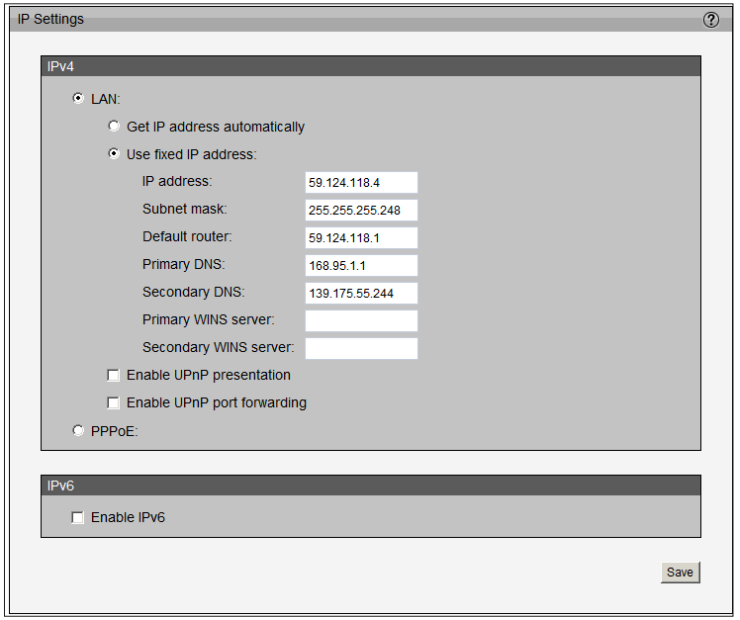
Default Router: This is the gateway used to forward frames to destinations in a different subnet. (Invalid router setting will cause the transmission to fail if its destination is in a different subnet).

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

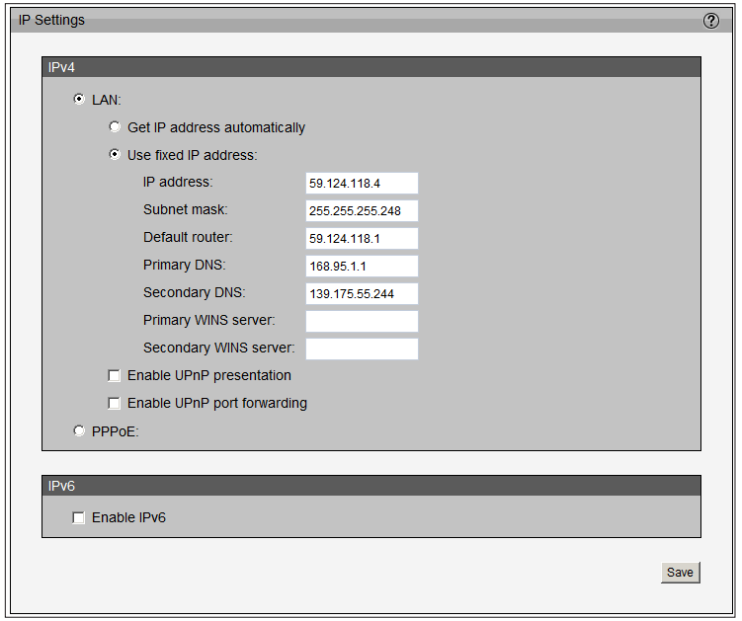
Secondary DNS: Secondary Domain Name Server (DNS) that backs up the Primary DNS.

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

Secondary WINS Server: The secondary WINS server that maintains the database for computer name and IP address.



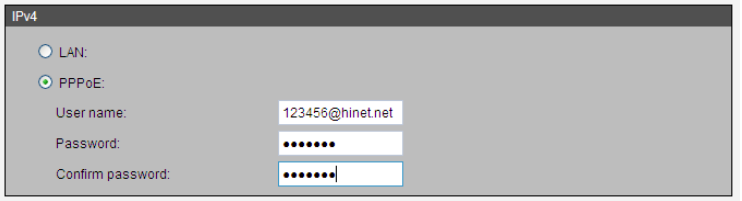
- **Enable UPnP Presentation:** Check the box to **Enable UPnP presentation** for the camera so that whenever a camera is added to the LAN, shortcuts of connected network cameras will be listed in *My Network Places*. You can click the shortcut to link to the web browser. (Currently, UPnP is supported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



How does UPnP work?

UPnP networking technology provides automatic IP configuration and dynamic discovery of devices added to a network. Services and capabilities offered by networked devices, such as printing and file sharing, are available without bothersome network configuration. For network cameras, you will see network camera shortcuts at *My Network Places*.

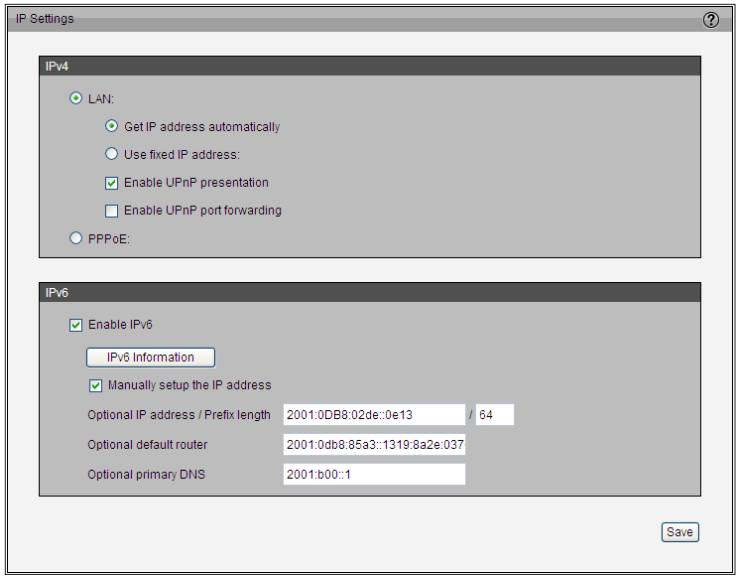
PPPoE: Select this option to configure the camera to make it accessible from anywhere with an Internet connection. To utilize this feature, you must have an account provided by your Internet Service Provider (ISP).



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

1. Set up the camera on the LAN
2. Go to **Live View > Setup > Event management > Event settings > Server Settings** (Refer to "Sever Settings" on page 54 to add a new e-mail or FTP server.)
3. Go to S**etup > Event management > Event settings > Media Settings** (Refer to "Media Settings" on page 56). 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.

IPv6



Enable IPv6: Check the box and click **Save** to **Enable IPv6**. This only works if your network environment and hardware support IPv6. Your browser should be Internet Explorer 7 or above, or Mozilla Firefox 3.5 or above.

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

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

Follow the steps below to link to an IPv6 address:

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

Manually Setup the IP Address: Check the box to manually configure IPv6 settings if your network environment does not have DHCPv6 server and advertisement-enabled routers.

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.

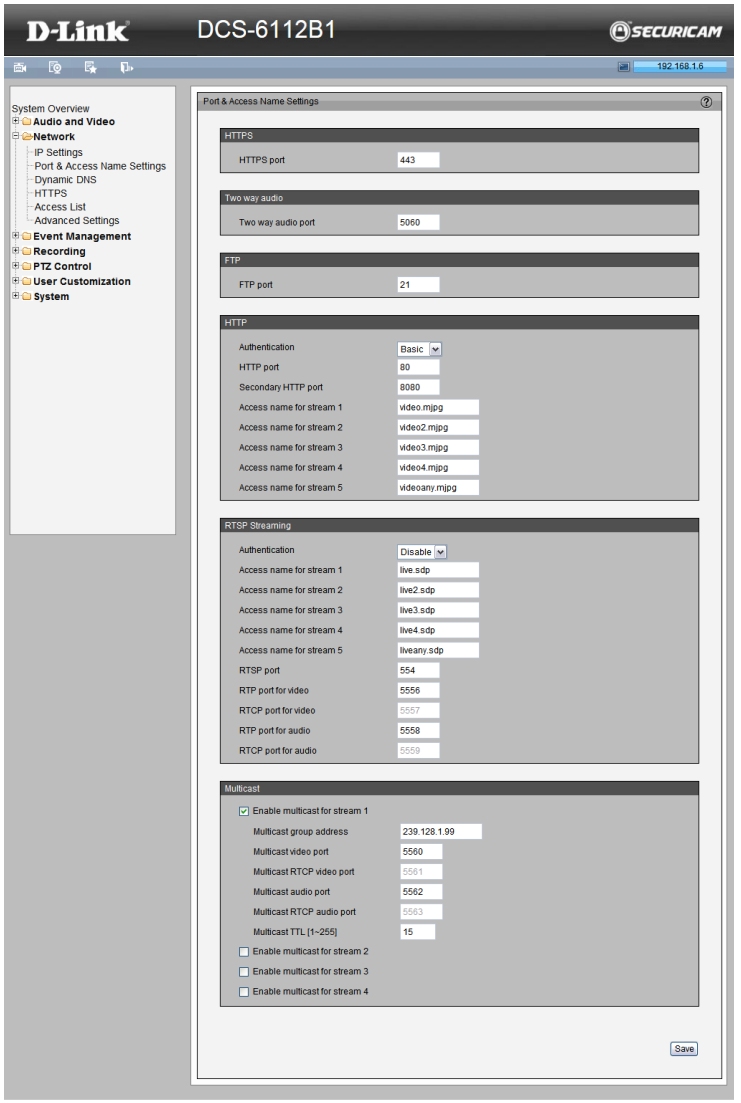
Two way audio
The *Two way audio port* is set to **5060** by default. It can also be assigned to another port number between 1025 and 65535.
This camera supports two way audio communication so that users can transmit and receive audio simultaneously.
By using the external microphone and an external speaker, users can communicate with people near the camera.

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. By default, the *FTP port* is set to **21**. It also can be assigned to another port number between 1025 and 65535.

HTTP
The *HTTP port* and *Secondary HTTP port* can also be assigned to another port number between 1025 and 65535.
To access the camera on the LAN, both the *HTTP port* and *Secondary HTTP port* can be used. For example, when the *HTTP port* is set to 80 and the *Secondary HTTP port* is set to 8080, you can access the camera using the example links below:

http://192.168.0.20 or http://192.168.0.20:8080



HTTP

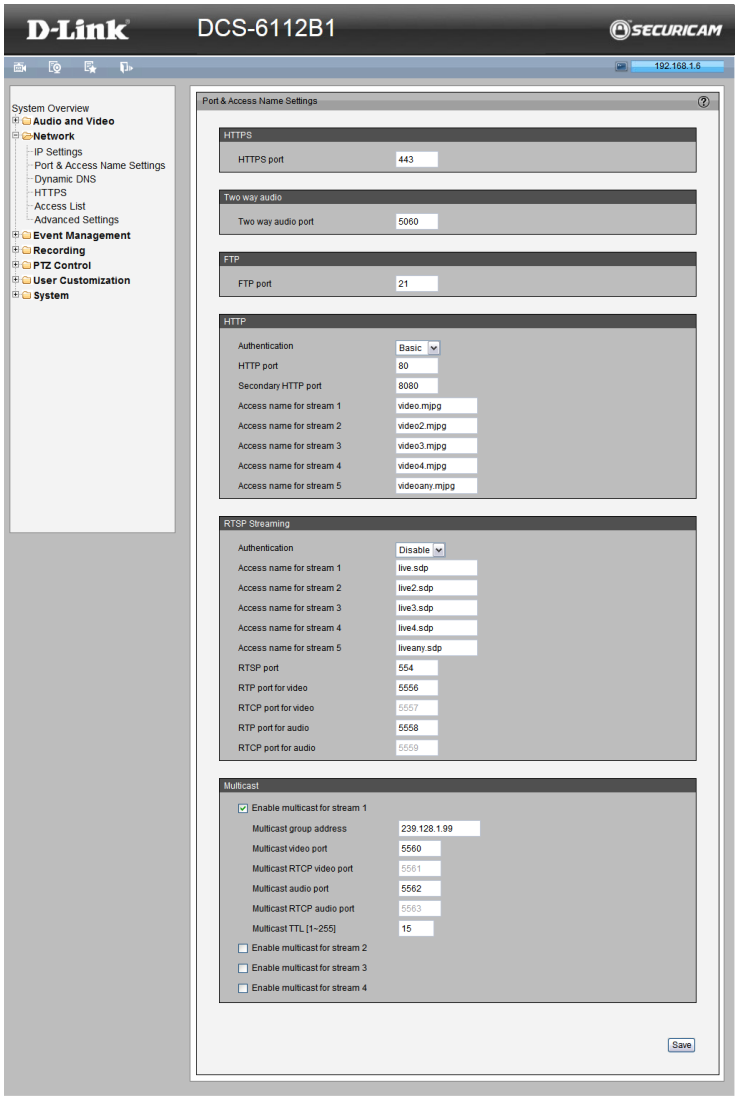
Authentication: Depending on your network security requirements, the camera provides two types of security settings for streaming via HTTP protocol: *basic* and *digest*. If **basic** authentication is selected, the password is sent in plain text format, but there can be potential risks of it being intercepted.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

Access name for stream 1 ~ 5: This camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. If you are using Mozilla Firefox to access the camera, when the video mode is set to JPEG, users will receive video comprised of continuous JPEG images This technology, known as "server push", allows the camera to feed live pictures to Firefox. Use the following HTTP URL command to request transmission of the streaming data:

For example: http://<ip address>:<http port>/<access name for stream 1 ~ 5>

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:
1. *Internet Explorer does not support "server push" technology. Therefore, if you attempt to use http://<ip address>:<http port>/<access name for stream 1 ~ 5>, you will fail to access the camera.*
2. *Stream 5 is a special stream. Users can only use URL commands to request stream 5.*



RTSP Streaming

Authentication: Depending on your network security requirements, the 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 ~ 5: This camera supports multiple streams simultaneously. The access name is used to differentiate the streaming source. If you want to use an RTSP player to access the camera, you have to set the video mode to **H.264 / MPEG-4** and use the following RTSP URL command to request transmission of the streaming data:
RTSP port /
RTP port for video, audio/
RTCP port for video, audio

- RTSP (Real-Time Streaming Protocol) controls the delivery of streaming media. By default, the port number is set to 554.
- The RTP (Real-time Transport Protocol) is used to deliver video and audio data to the clients. By default, the RTP port for video is set to 5556 and the RTP port for audio is set to 5558.
- The RTCP (Real-time Transport Control Protocol) allows the Network Camera to transmit the data by monitoring the Internet traffic volume. By default, the RTCP port for video is set to 5557 and the RTCP port for audio is set to 5559.

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

Multicast:
Check the boxes to enable multicast for stream(s) 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.

When you enable multicast streams, the detailed configuration information will be displayed for each:

Multicast group address: Displays the *Multicast group address* for the enabled multicast stream.

Multicast video, audio port/ Multicast RTCP video, audio port: The port numbers can be changed to values between 1025 and 65535. The first multicast port listed (RTP port) must be an even number, and the other multicast port number (RTCP) is the multicast RTP port number plus one, and thus will always be an odd number. When the multicast RTP port changes, the corresponding 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 (DDNS) for the camera. This service allows your camera to have a fixed host and domain name.

Enable DDNS: Check the box to **Enable DDNS**.

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 as described below:

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

User name: Enter your **User name** or e-mail used to connect to the DDNS

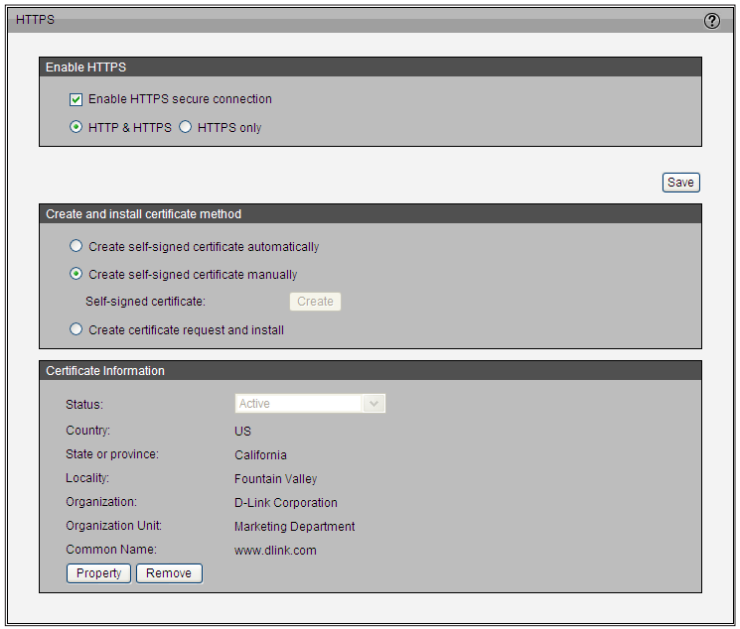
Password: Enter your **Password** used to connect to the DDNS server.

Status: Displays the connection *Status*, which is automatically determined by the system.

Click **Save** to save your settings.

HTTPS

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



Enable HTTPS
Check the box to **Enable HTTPS secure connection**. Then select a connection type: **HTTP & HTTPS** or **HTTPS only**. You must first create and install a certificate in the second column before you click the **Save** button.

Create and Install Certificate Method
Before using HTTPS for communication with the camera, a certificate must be created. 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**. Security Alert dialog windows will pop up. Click **OK** or **Yes** to enable HTTPS.

Create Self-signed Certificate Manually
1. Click **Create** to open the *Create Certificate* page. Click **Save** to generate the certificate.
2. *Certificate Information* will be displayed in the third column as shown to the right. Click **Property** to view more detailed information about the certificate.

Create Certificate Request and Install
Select this option to create a certificate from a certificate authority.

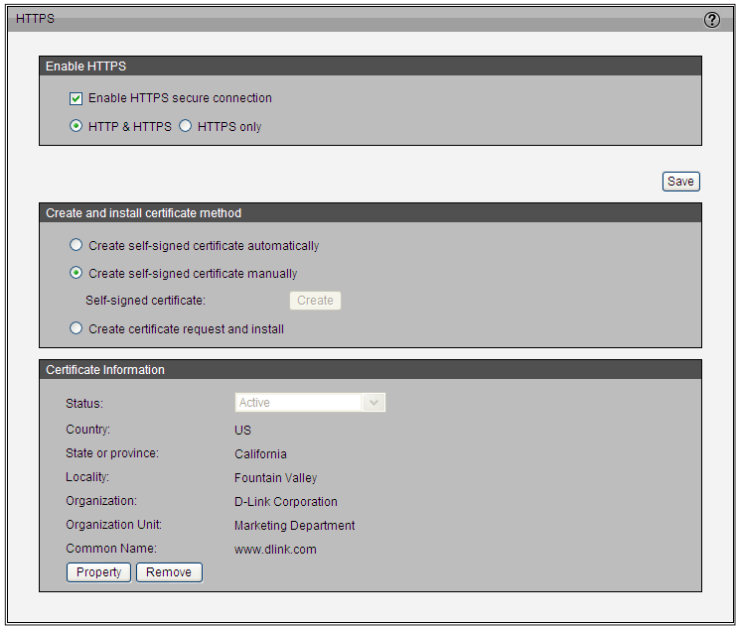
1. Click **Create** to open the **Create Certificate** page, then click **Save** to generate the certificate.
2. If you see the information bar, click **OK** and click on the Information bar at the top of the page to allow pop-ups.
3. The pop-up window shows an example of a certificate request.
4. Look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

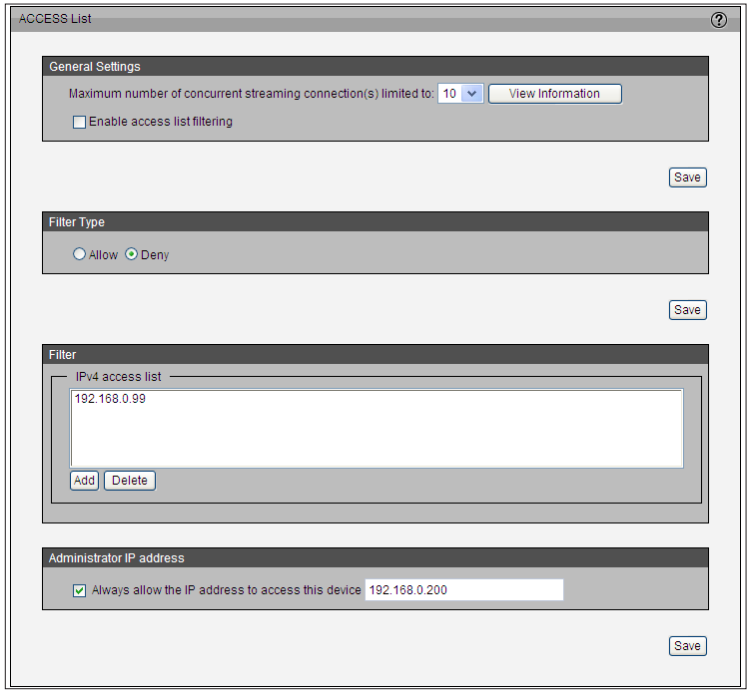
1. Uncheck **Enable HTTPS secure connection** in the first column and click **Save.** A warning dialog will pop up.
2. Click **OK** to **disable HTTPS**.
3. The web page will redirect to a non-HTTPS page automatically.

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



Access List

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

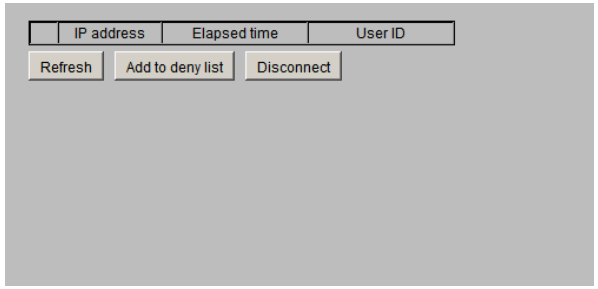


General Settings

Maximum number of concurrent streaming connection(s) limited to: You may select 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. Internet Explorer or Quick Time Player).

View Information: Click this button to display the *Connection Status* window, which will display 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 set a password for the web page, clients must enter a **User name** and **Password** to access the live video. The user name will be displayed in the *User ID* column. If the administrator allows clients to link to the web page without a user name and password, the *User ID* column will be empty.



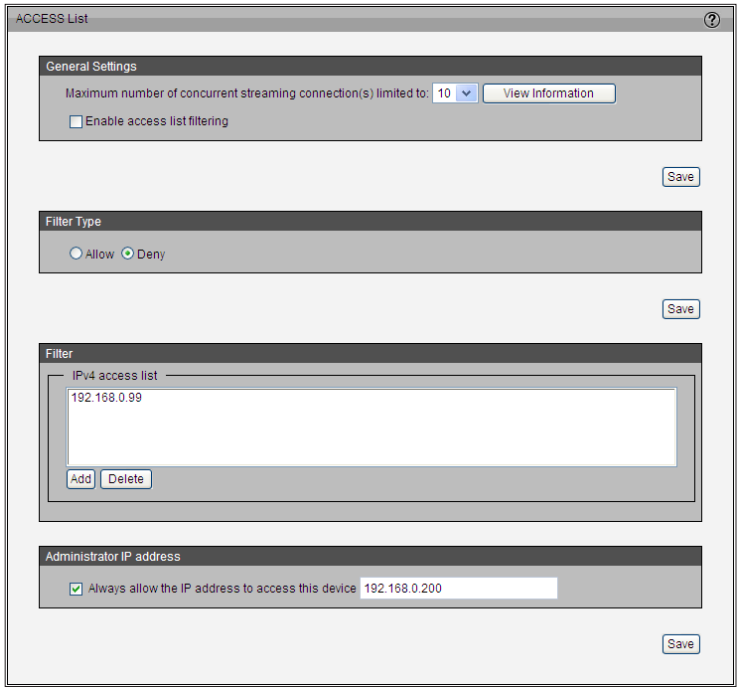
There are some situations that allow clients access to the live video without a user name and password:

1. If 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" on page 66.
2. If the administrator set up a user password, and then set *RTSP Authentication* setting to **disable**.

Buttons:

- **Refresh:** Click 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. The selected connections will only be disconnected temporarily and will automatically try to re-link again (i.e. Internet Explorer or Quick Time Player). If you want to enable the denied list, check **Enable access list filtering** and click **Save**.
- **Disconnect:** If you want to break off the current connections, select them and click the **disconnect** button. The selected connections will only be disconnected temporarily and will automatically try to re-link again (i.e. Internet Explorer or Quick Time Player).

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



Filter Type

Select **Allow** or **Deny** for the filter type. If you select **Allow**, only clients with IP addresses on the *IPv4 Access List* below will be able to access the camera. On the other hand, if you choose **Deny**, clients with IP addresses on the *IPv4 Access List* below will not be allowed to access the camera.

Filter

Click **Add** to add a rule to the *IPv4 Access List*. Note that the IPv6 access list column will not be displayed unless you enable IPv6 on the Network page. For more information about IPv6 Settings, refer to "IPv6" on page 39.

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: Check the box and then add the Administrator's IP address in the provided field to make sure the Administrator can always connect to the device.

Advanced Settings

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

The SNMP consists of the following three key components:

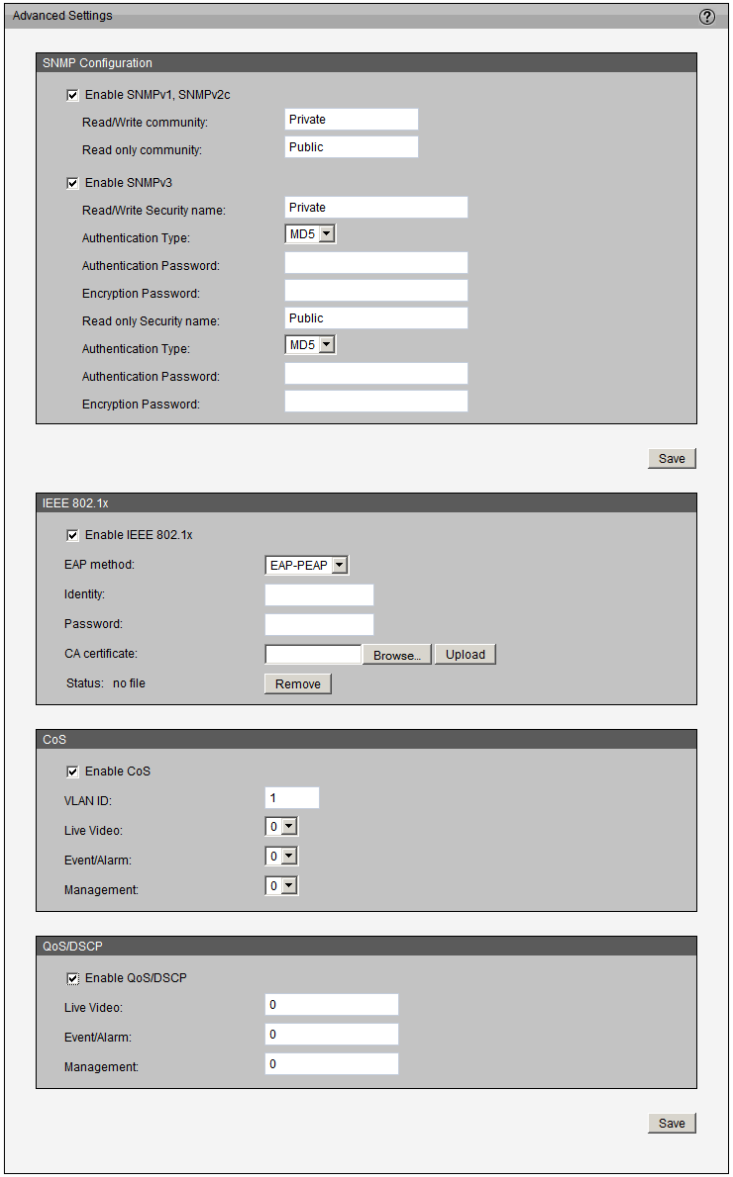
1. **Manager:** Network-Management Station (NMS), a server that runs applications to monitor and control managed devices.
2. **Agent:** A network-management software module on a managed device which transfers the status of managed devices to the NMS.
3. **Managed device:** A network node on a managed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

Enable SNMPv1, SNMPv2:
Before configuring SNMP settings, first enable your NMS. Check the box to **Enable SNMPv1, SNMPv2c**. Enter the names of **Read/Write community** and **Read Only community** according to your NMS settings.

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

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

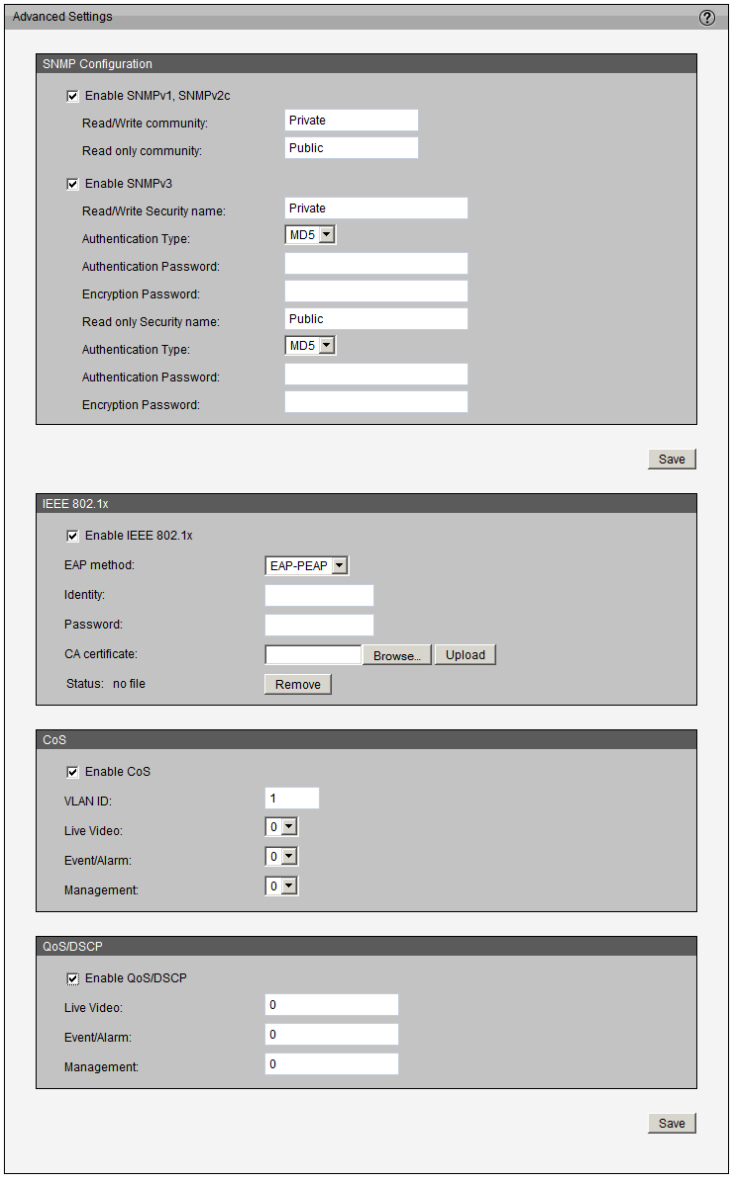
IEEE 802.1x
Check the box to enable if your network environment uses IEEE 802.1x, which is a port-based network access control. The network devices, intermediary switch/access point/hub, and RADIUS server must support and enable 802.1x settings.



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

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) that can be validated by a RADIUS server.
2. Connect the camera to a PC or notebook outside of the protected LAN. Open the configuration page of the camera as shown below. Select an **EAP method**, **EAP-PEAP** or **EAP-TLS**. In the fields below, enter your **Identity** (ID) and **Password** issued by the CA, then upload related certificate(s).
3. When all settings 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) Defined:

QoS refers to a resource reservation control mechanism, which guarantees a certain quality to specific services on the network. QoS 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 can use, and thus provide higher reliability and stability on the network.

Requirements for QoS:

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

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

CoS

IEEE802.1p defines a QoS model at OSI Layer 2 (Data Link Layer), which is called CoS (Class of Service). It adds a three-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.

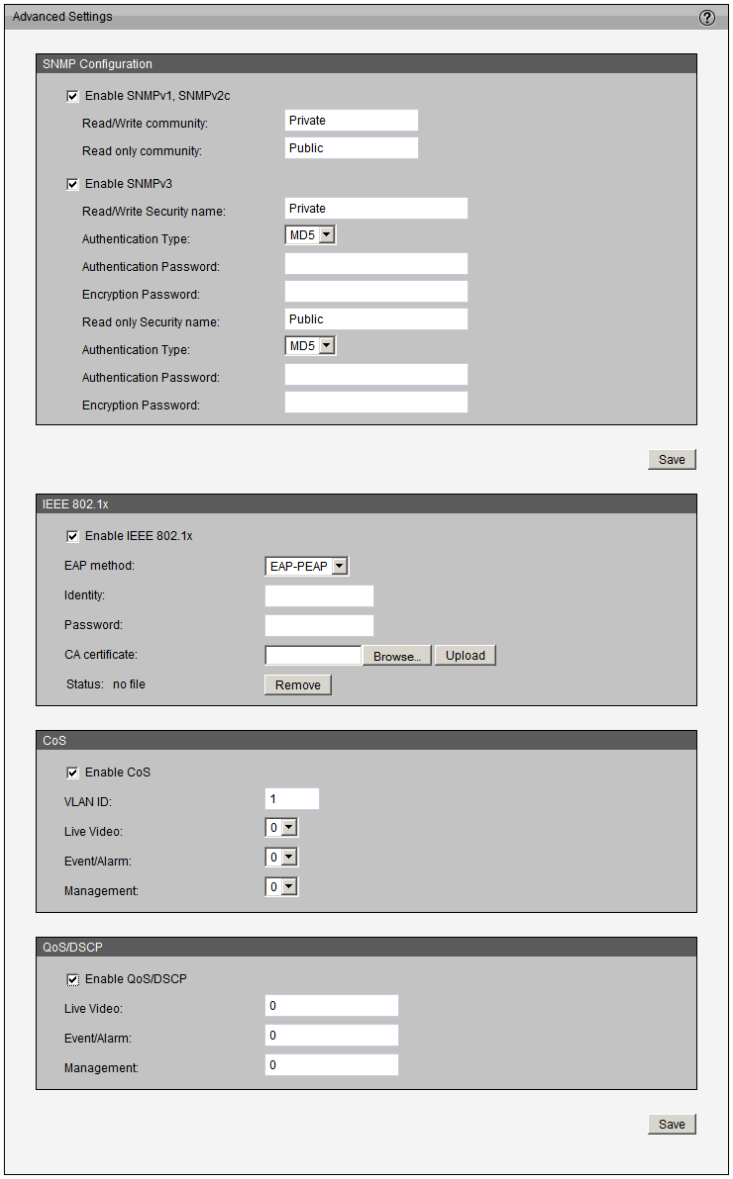
Follow the steps below to enable CoS settings:
1. Check the box to **Enable CoS**
2. Enter the **VLAN ID** of your switch (0~4095)
3. Select a priority for each application (0~7).

Notes:

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

QoS/DSCP

Check the box to **Enable 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. This indicates how a given packet should be forwarded, and is also referred to 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, determining how much bandwidth should be reserved.



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: Check the box to turn on motion detection.

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

Sensitivity: Set a percentage for 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.

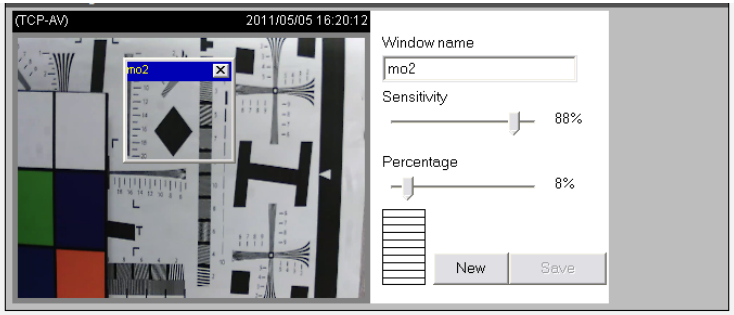
Note: *Setting a higher sensitivity and a lower percentage will make motion easier to be detected.*

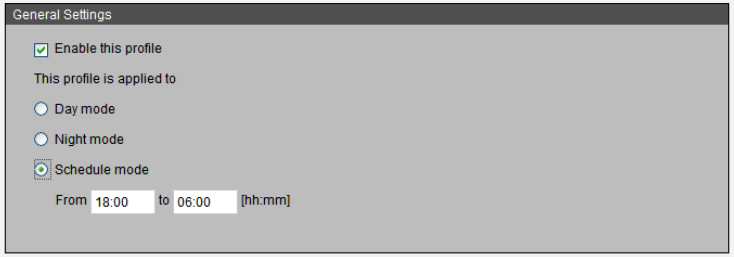
Click **New** to add a new window. A maximum of three motion windows can be opened simultaneously. Use your mouse to drag the window frame to resize it, or the title bar to move it. Click on the **X** at the upper right corner of the window to close it.

Click **Save** to save your 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 bars.
4. Click **Save** to apply the changes.
5. Check the box to **Enable motion detection**.





Profile:

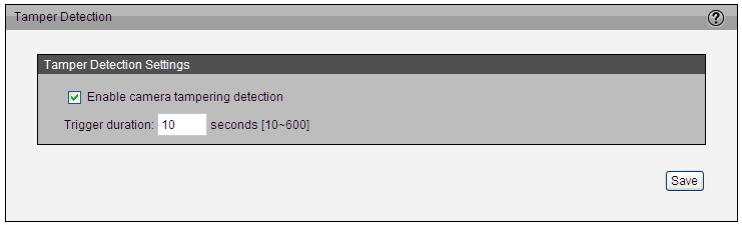
You can configure two sets of sensor settings:

For example, you could use *Profile 1* for normal situations, and *Profile 2* for special situations that may require **Schedule mode** or **Night mode***.

* Night mode applies to the DCS-6113 only.

Tamper Detection

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



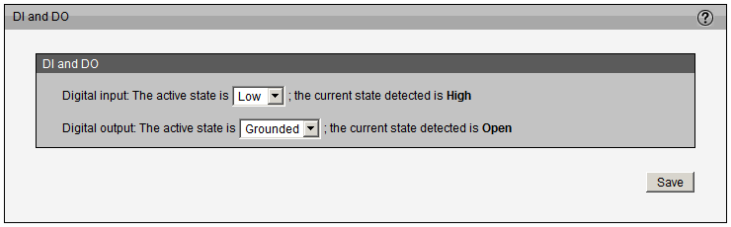
To enable tamper detection, follow the steps below:

1. Check the box to **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.

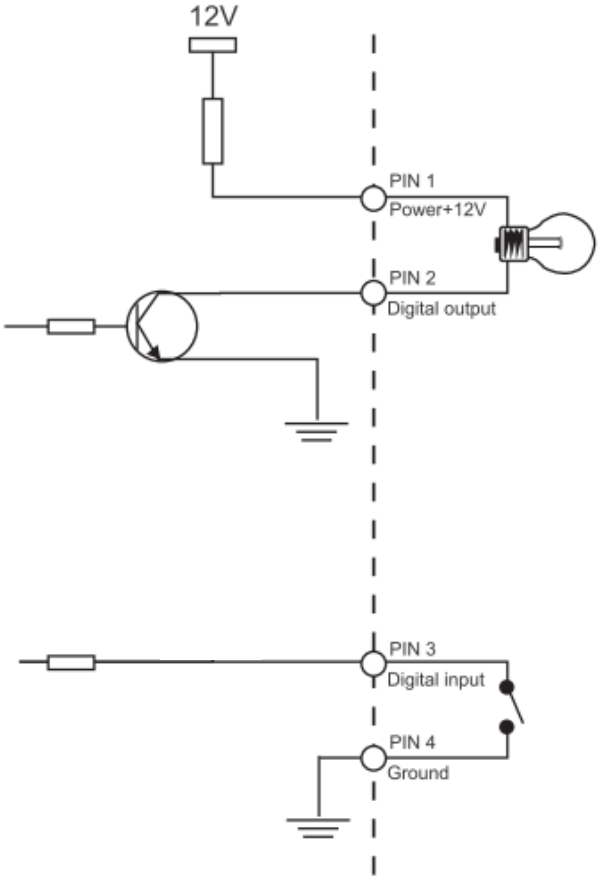
Set up the event source as Camera Tampering Detection on **Event Settings** > **Server Settings** (how to send alarm message)/ **Media Settings** (send what type of alarm message). Refer to "Event Settings" on page 54.

DI and DO

The DCS-6112/DCS-6113 provides a general I/O terminal block with one digital input and digital output for device control. The I/O connector provides the physical interface for digital input (DI+, GND) and digital output (DO-, +12V) that is used for connecting a diversity of external alarm devices to the camera such as IR-Sensors and alarm relays. Once triggered images will be taken and e-mailed.

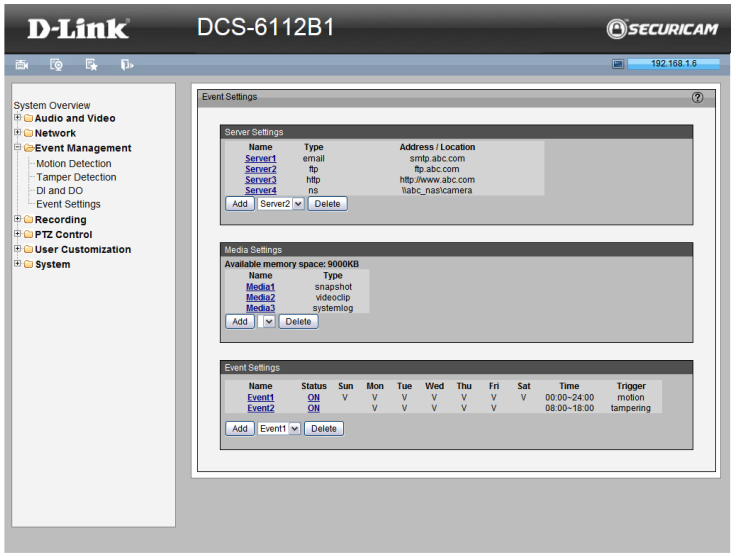


DI/DO Schematics



Event Settings

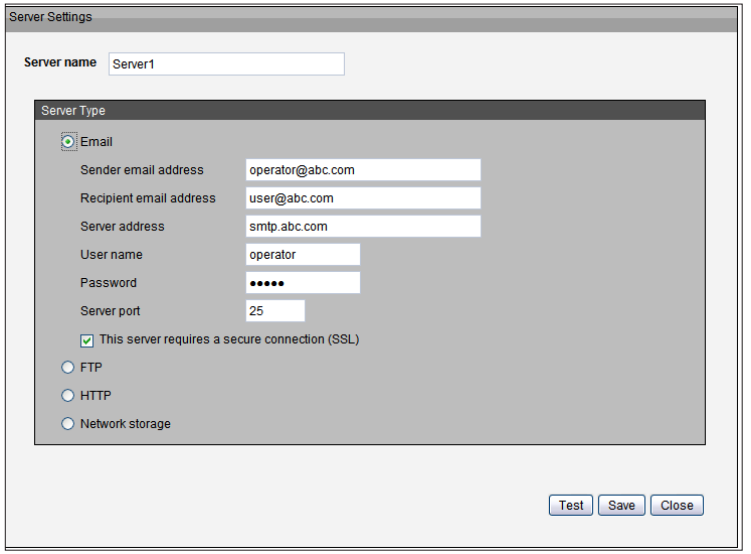
This section explains how to configure the camera to respond to particular situations (events). A typical scenario is when a motion is detected, the camera sends buffered images to an FTP server or to an e-mail address as notification.



Sever Settings

Click **Add** on *Event Settings* page to open the **Server Settings**. You can specify where the notification messages should be 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: **E-mail**, **FTP**, **HTTP**, and **Network storage**. Select one to display the corresponding configuration options. You may configure just one or all four of them.



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

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

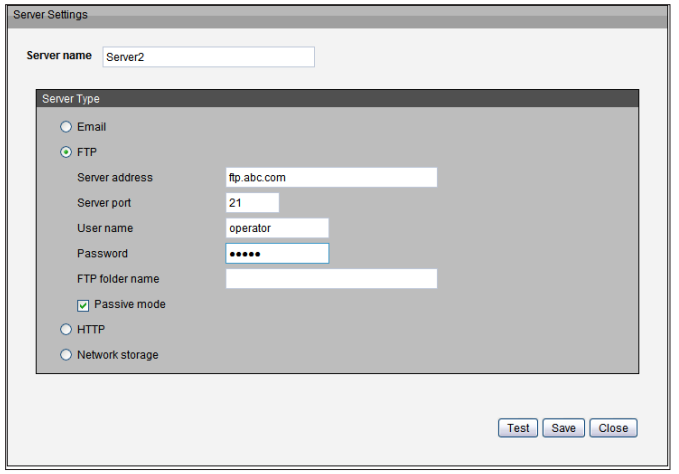
If your SMTP server requires a secure connection (SSL), check the box by **This server requires a secure connection (SSL)**.

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 results of your test.

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, check the box to enable passive mode FTP and allow data transmission to pass through the firewall.

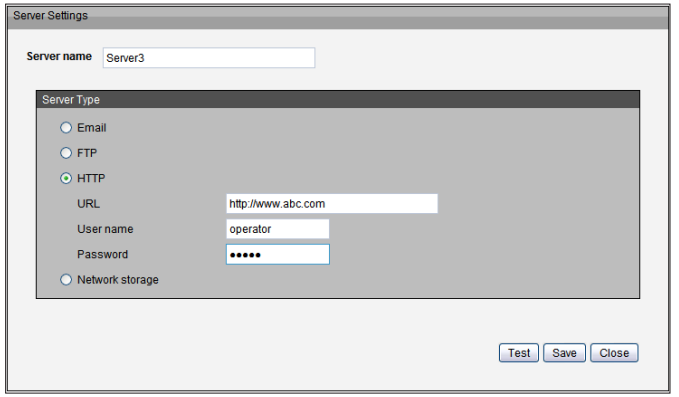


To verify if the FTP settings are correctly configured, click **Test**. The results will be shown in a pop-up window. If successful, you will also receive a test.txt file on the FTP server.

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

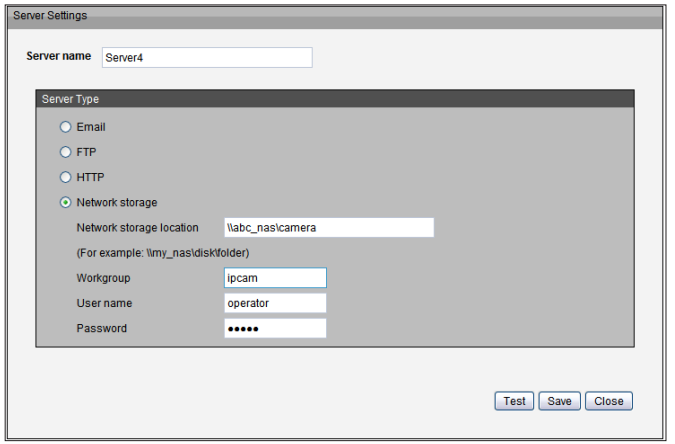
HTTP: Select to send the media files to an HTTP server when a trigger is activated.

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



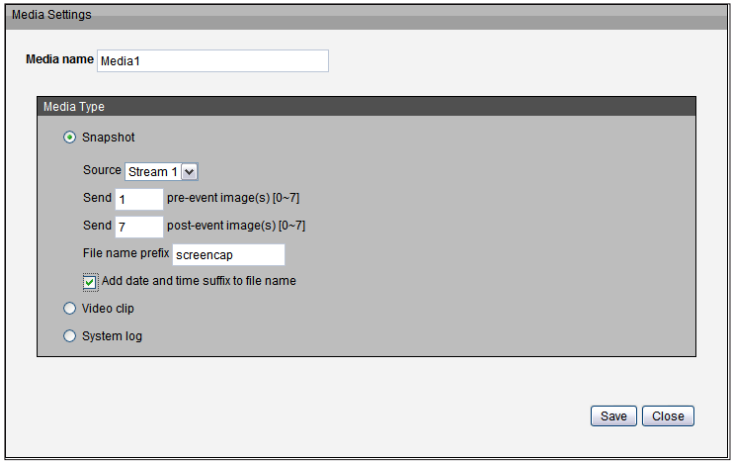
To verify if the HTTP settings are correctly configured, click **Test**. The results will be shown in a pop-up window. If successful, you will receive a test.txt file on the HTTP server.

Network storage: Select to send the media files to a network storage location when a trigger is activated.



Click **Save** to enable the settings then click **Close** to exit the page. When completed, the new server settings will automatically be displayed on the *Event Settings* page.

Media Settings



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

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 one to display the corresponding configuration options. You can configure one or all three of them.

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

Source: Select a source for taking snapshots, from streams 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 seven 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 seven 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: Check the box to add a date/time suffix to the file name.

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

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

Source: Select a source for video clips, from streams 1 ~ 4.

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 nine seconds can be set.

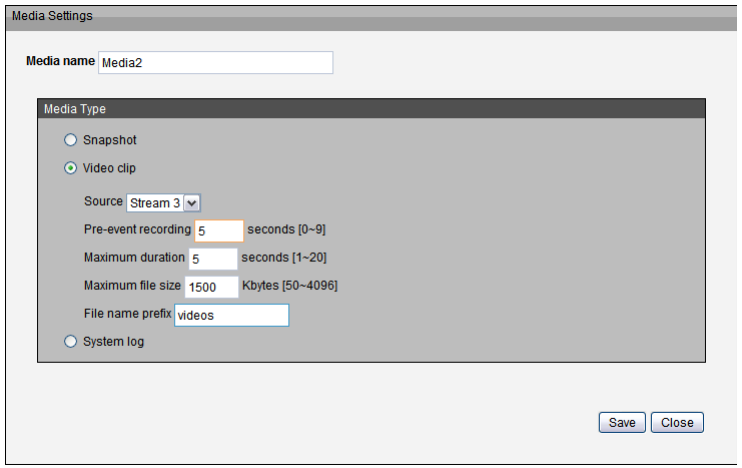
Maximum duration: Specify the maximum recording duration in seconds. Up to 20 seconds can be set. For example, if pre-event recording is set to five seconds and the maximum duration is set to 10 seconds, the camera continues to record for another four seconds after a trigger is activated.

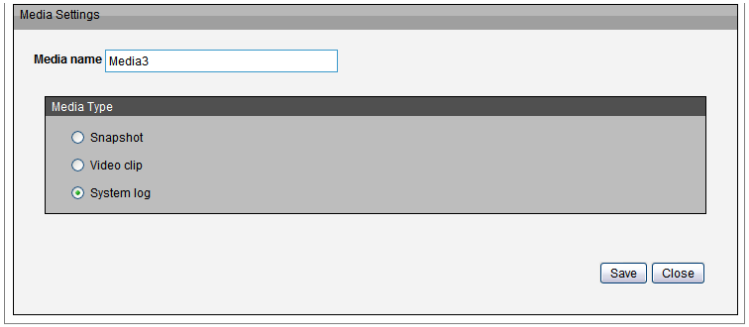
Maximum file size: Specify the maximum file size allowed.

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

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

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

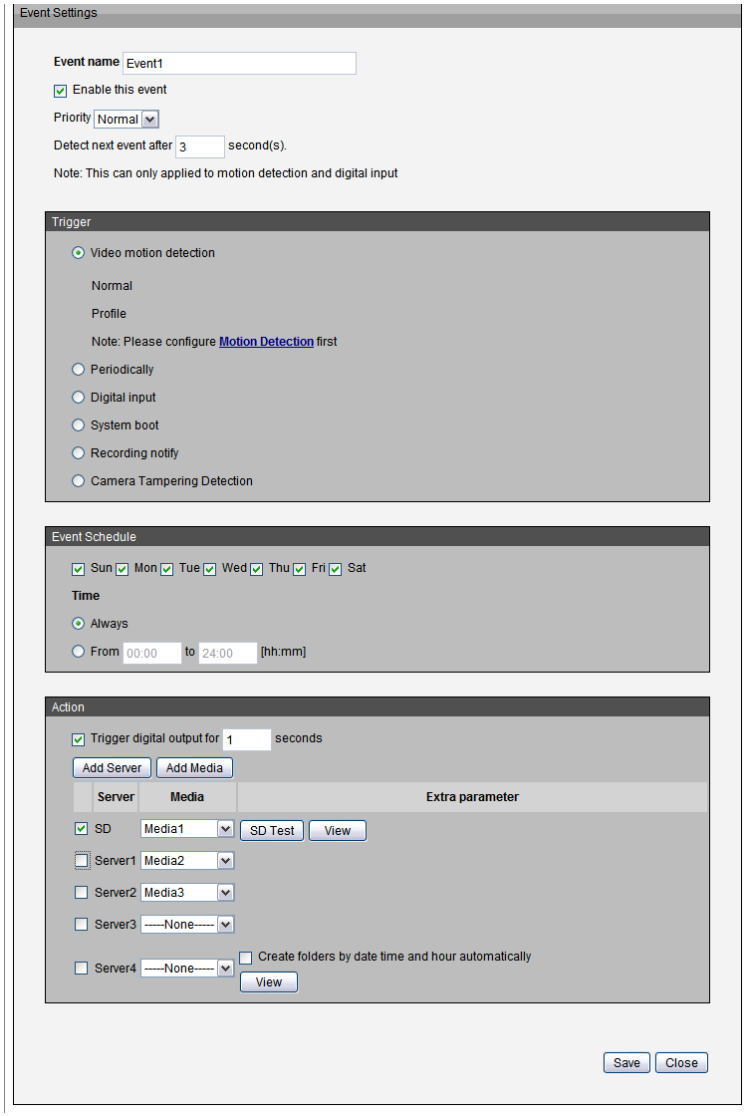
Under *Event Settings*, click **Add** to open the *Event Settings* page. You can arrange three elements -- **Trigger**, **Schedule**, and **Action** to define an event. A total of three event settings can be configured.

Event name: Enter a name for the event.

Enable this event: Check the box 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 used for both events of motion detection and digital input trigger.



Trigger

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

Video motion detection: This option makes use of the built-in motion detection mechanism as a trigger. To enable this function, you need to first configure a Motion Detection Window. For more information, refer to "Motion Detection" on page 51.

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

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

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

Recording notify: This option allows triggers an event when the recording disk is full or when recording starts to rewrite older data.

Camera Tampering Detection: This option triggers an event when the camera detects that it is being tampered with. To enable this function, you need to configure the Tamper detection option first. Refer to "Tamper Detection" on page 52.

Event Schedule

Specify the period for the event

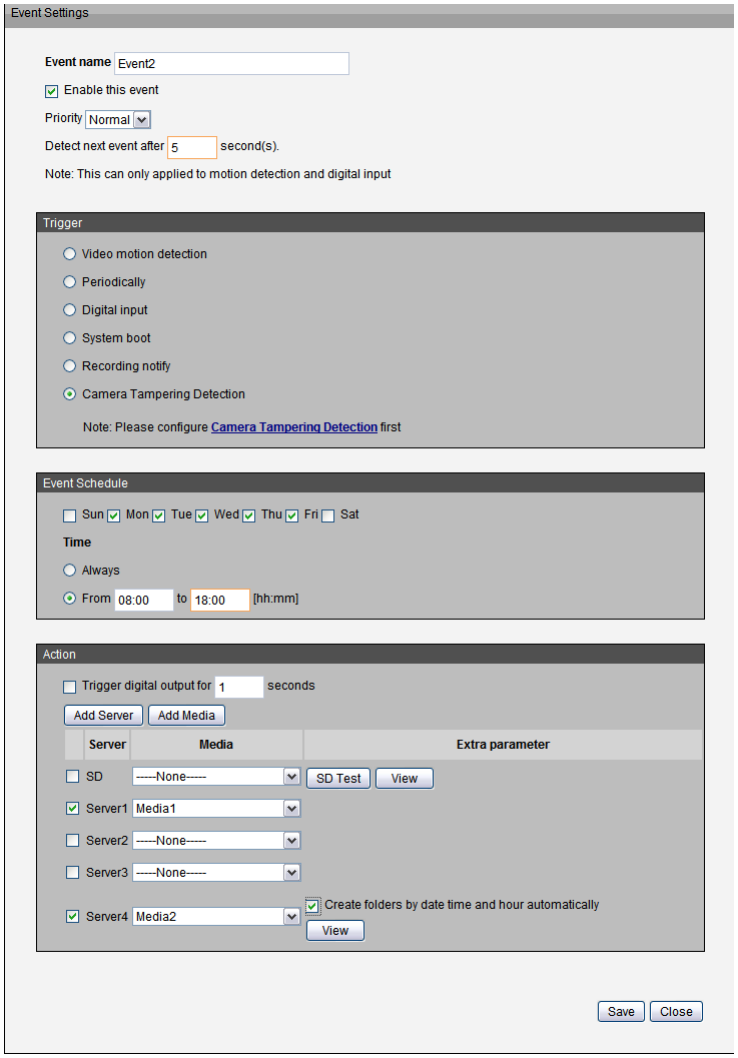
1. Select the day(s) of the week.
2. Choose a time. Select **Always**, or enter the recording schedule in 24-hr time format.

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 settings so that the camera will know what action to take (i.e. specify the server to send the media files to) when a trigger is activated.

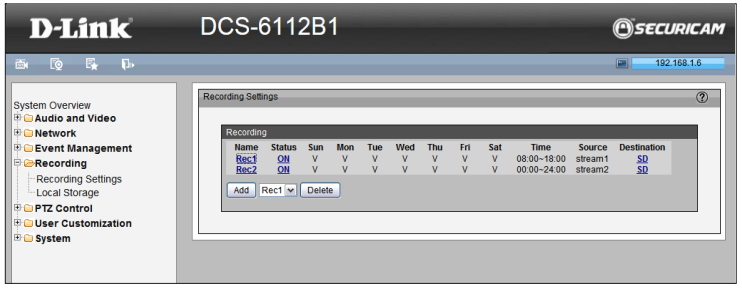
- **Add Server:** same as Server Settings
- **Add Media:** same as Media Settings



Recording

Recording Settings

Click **Add** to open the *Recording Settings* page. You can define the recording source, recording schedule, and recording capacity. A total of two recording settings can be configured.



Recording name: Enter a name for the recording.

Enable this recording: Check the box to enable video recording.

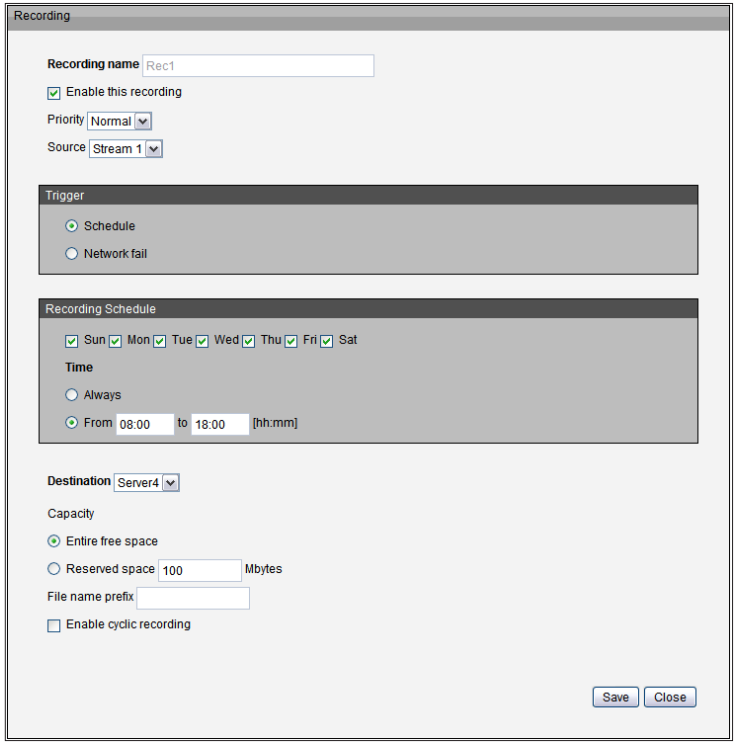
Priority: Select the relative importance of this recording setting (**High**, **Normal**, or **Low**).

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

Trigger: Select a trigger source. If **Schedule** is selected, the server will record files on the network storage (NAS) according to a set schedule.

Recording Schedule: Specify the recording duration.

1. Select the day(s)of the week.
2. Choose a time. Select **Always**, or enter the recording schedule in 24-hr time format.



Destination: You can select a destination -- either 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.

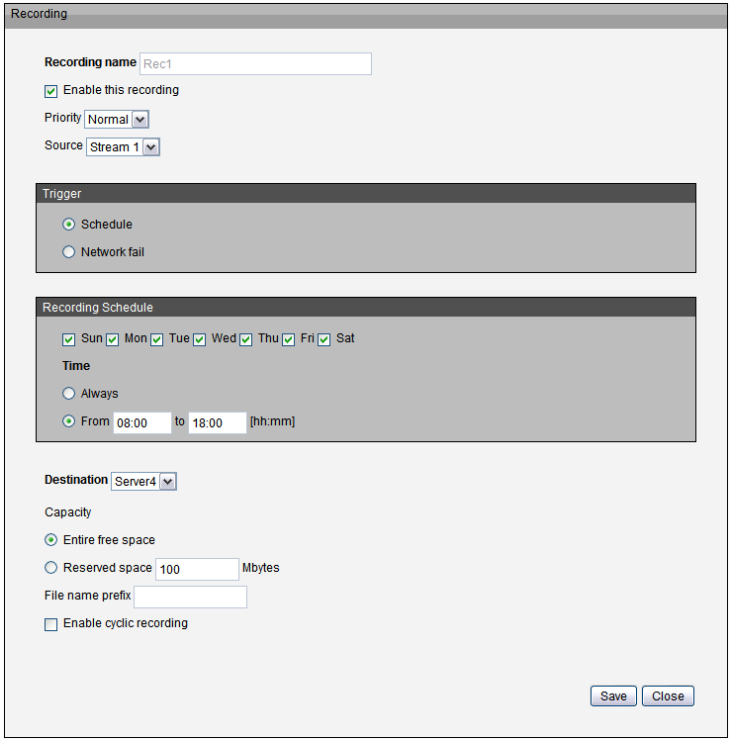
Enable cyclic recording: If you check this box, when the maximum capacity is reached, the oldest file will be overwritten by the latest one. The reserved amount is reserved for cyclic recording to prevent malfunction. This value must be larger than 15 Mbytes.

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

When completed, check the box to **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.

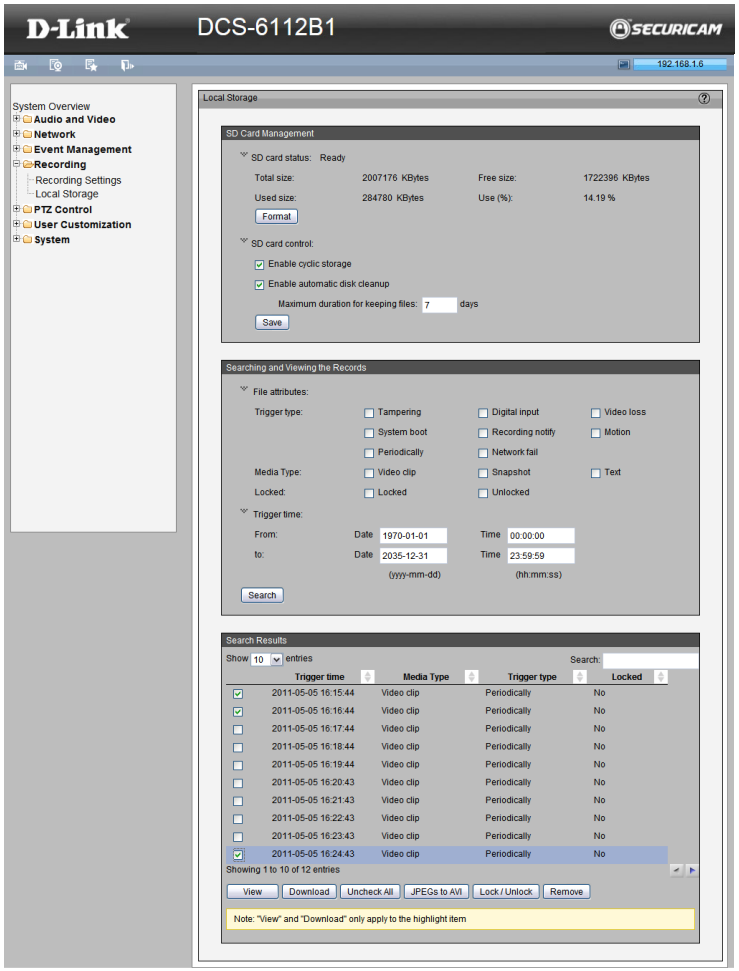
The new recording name will appear in the drop-down list on the recording page.

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 camera. 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. Remember to format the SD card when using it for the first time.

SD card control:
Check the box to **Enable cyclic storage**. When the maximum capacity is reached, the oldest file will be overwritten by the latest one.

Check the box to **Enable automatic disk cleanup** and enter the number of days you wish to retain a file. For example, if you enter **7** days for **Maximum duration for keeping files** , the recorded files will be stored on the SD card for seven 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: Enter the date and time range you want to search. Click **Search** and the recorded data corresponding to the search criteria will be listed in *Search Results* Window.

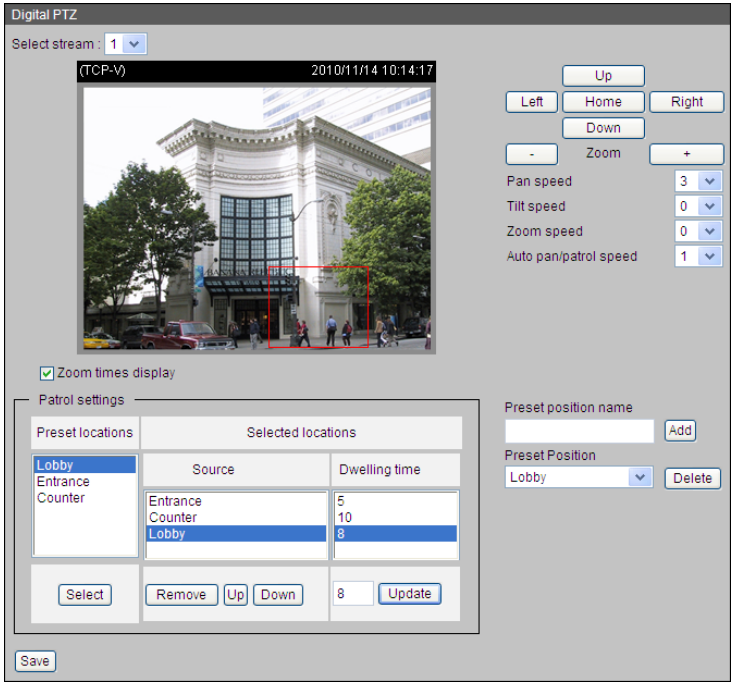
Search Results

This area will display 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.

PTZ Control

Digital PTZ

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



Follow the steps below to preset a position:

1. Adjust the shooting area to the desired position using the direction 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 settings. The preset positions will be displayed under the *Preset Locations* list on the left-hand side.
3. To add additional preset positions, please 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. Refer to the illustration on the next page.
6. Click **Save** to enable the settings. The Preset Positions will also be displayed on the Live Video. Select one from the drop-down list and the camera will move to the selected preset position.

Patrol Setting

You can select some preset positions for the camera to patrol.
Please follow the steps below to set up a patrol schedule:

1. Click a preset location on the list and click **Select**.
2. The selected preset location will be displayed on the *Source List*.
3. Set the **Dwelling time** for the preset location during auto patrol. You can also manually enter a value in the **Dwelling time** field 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 settings.

User Customization

Live Video Page Configuration

Preview: Displays the new layout of Logo/Background/Title based on user settings.

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

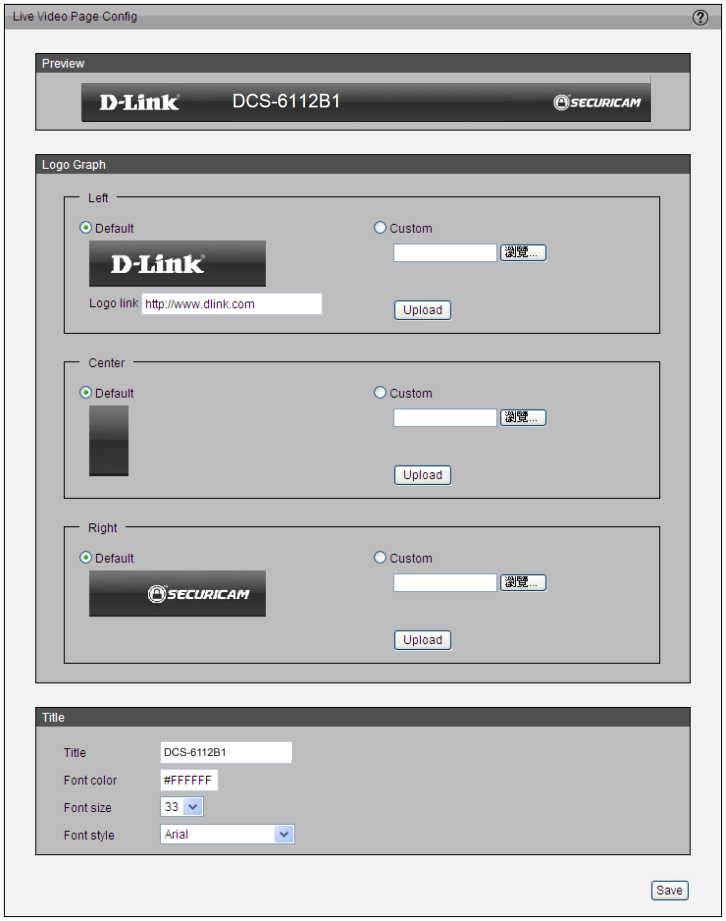
1. Click **Custom** and the **Browse** field will appear.
2. Select a logo from your files.
3. Click **Upload** to replace the existing logo with a new one.
4. Enter a website link if necessary.
5. Click **Save** to enable the setting.

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

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

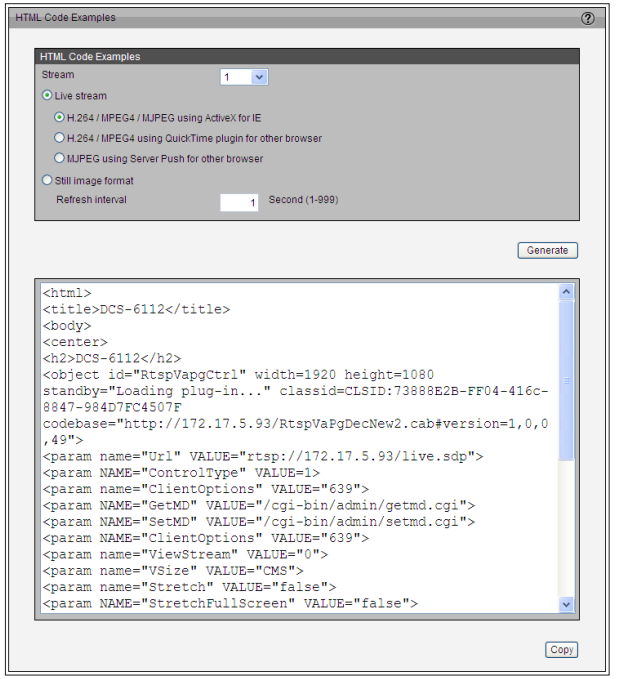
Click **Save** to enable the settings.

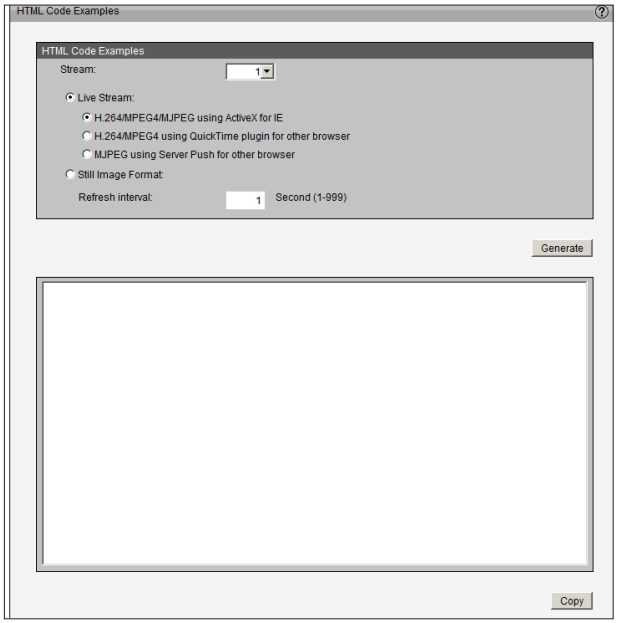
Title: You can enter a **Title**, **Font color**, **Font size**, and/or **Font style** to change the title at the top of your Live Video page.



HTML Code Examples

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





Stream:
Select from streams 1 to 4. Based on the profile of selected stream, the code will be generated accordingly. Up to 10 clients are supported for Live View.

Live Stream:

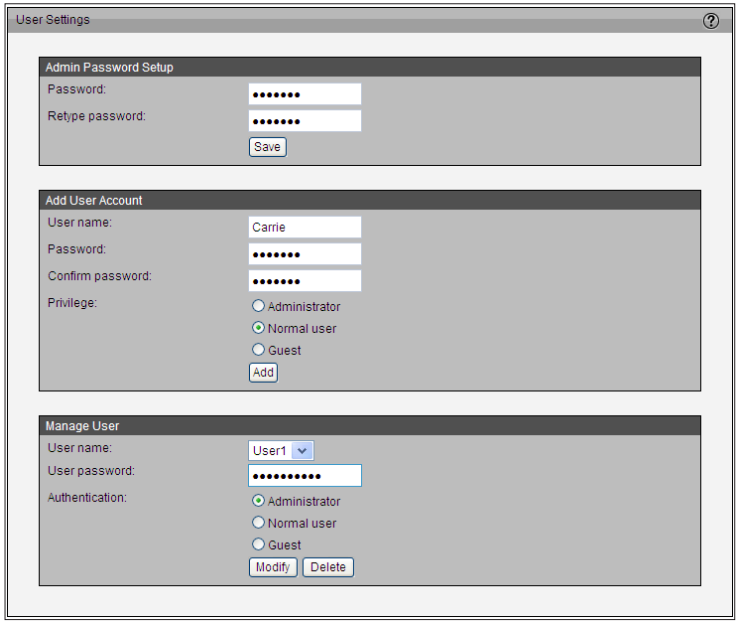
- **H.264/MPEG4/MJPEG using ActiveX for IE:**
  If target remote user client uses Internet Explorer(IE), then the example code can support H.264, MPEG4 and MJPEG stream.
- **H.264/MPEG4 using QuickTime plug-in for other browser**
  If target remote user client uses QuickTime plug-in for the browser,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

Still Image Format:

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

System
User Settings

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



Admin Password Setup:
The administrator account name is "admin", which is permanent and cannot be deleted. The default password is blank.

Add user account: Add a new user account.

User name: Enter a user name for the new account.

Password: Enter a password for the new account.

Privilege: Select the access rights for the new user.

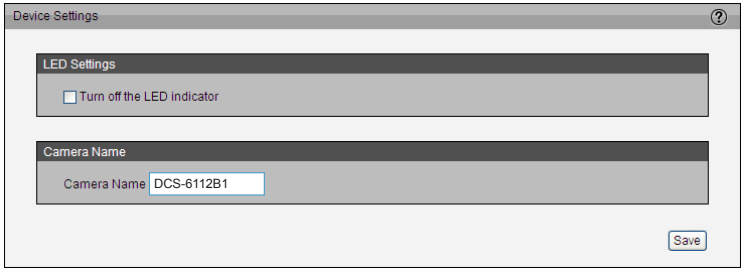
Manage user: Manage the accounts for existing users.

Authentication: Select access rights for existing users.

Device Settings

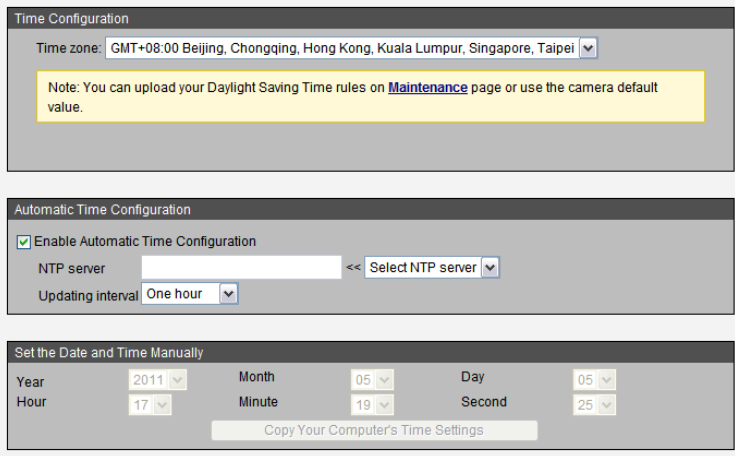
Turn off the LED indicator: Check the box to turn off the LED next to the lens. This will prevent anyone from observing the operation of the network camera.

Camera Name: Create a unique name for your camera.



Time and Date

You can automatically or manually configure, update, and maintain the internal system clock for your camera.



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

Note: *If you select a time zone with Daylight Saving Time, you will have the option to enable and configure DST.*

Enable Automatic Time Configuration: Check the box to enable this feature, in order 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.

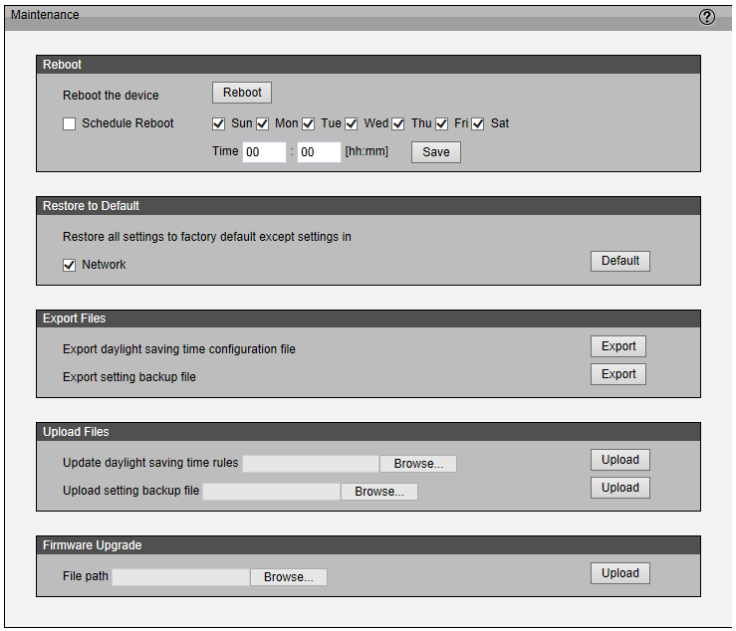
Updating Interval: The time interval for updating the time information from NTP server.

Set the date and time manually: Set the time and date manually. (Enter the **Year**, **Month**, **Day**, **Hour**, **Minute**, and **Second**.)

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

Maintenance

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



Reboot: Click to reboot the camera, which takes about one minute to complete. When completed, the Live Video page will be displayed in your browser. The following message will be displayed during the reboot process:

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

Restore all settings to factory default except settings in: Click **Default** to restore the camera to factory default settings. (If the check box by **Network** contains a check mark, the network settings will be saved when all other settings are set to factory default settings.)

Export/Upload Files: There are various options available for exporting and uploading files as detailed below:

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

Follow the steps below to export:

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

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

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

Upload setting backup file: Click **Browse…** to upload a setting backup file. 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 that you upload a settings backup file.

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

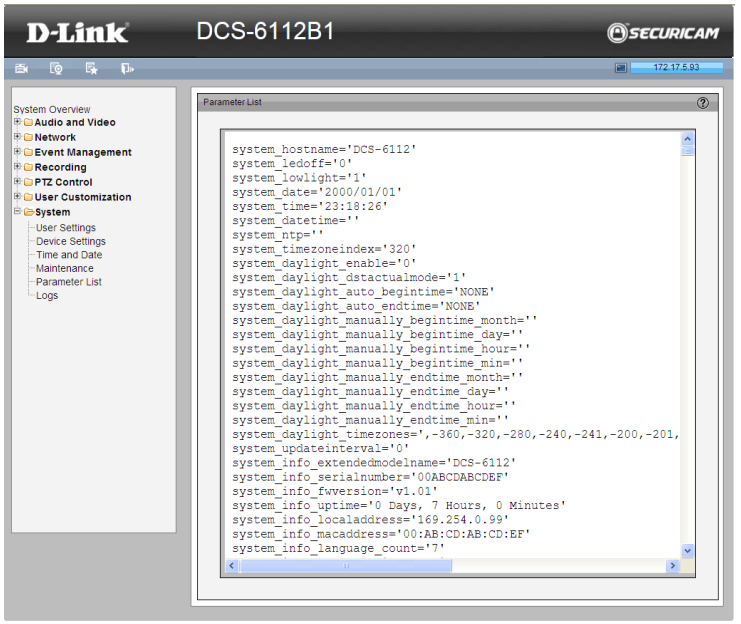
Note: *Do not power off the camera during the upgrade!*

Follow the steps below to upgrade the firmware:
1. Download the latest firmware file from the D-Link website. The file is in .pkg file format.
2. Click **Browse…** and select 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 this message:
Reboot system now!! This connection will close.
After that, you may re-access the camera.

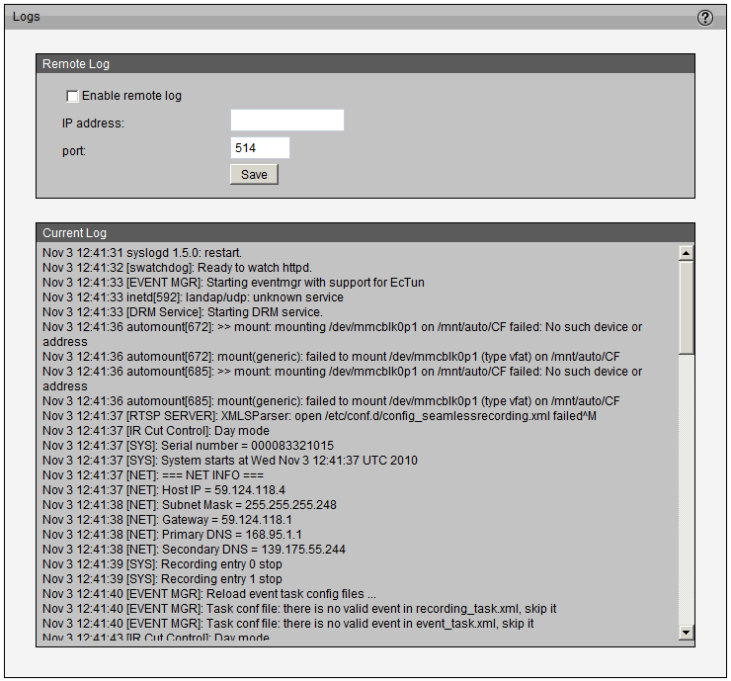
Parameter List

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



Logs

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



Enable 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 first a log-recording tool be installed on the remote server to receive system log messages from the camera. Be sure to note the IP address of the remote server.

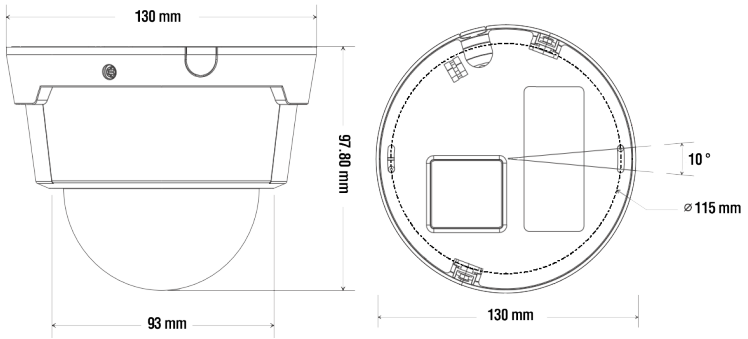
Follow the steps below to set up the remote log:

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, check the box to **Enable remote log**.
4. Click **Save** to save your settings.

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

Technical Specifications

Camera	Hardware Profile	▪ 1/2.7" Full HD progressive megapixel CMOS sensor ▪ Fixed lens, 4 mm F1.5 ▪ Digital Zoom 16X ▪ 15 meter IR illumination distance (DCS-6113, DCS-6113V) ▪ Shutter speed: 1/5 - 1/32,000 seconds	▪ Minimum Object Distance 100 cm ▪ Angle of view: (H) 77.4°, (V) 45.1°, (D) 88° ▪ Minimum illumination: 0.12 lux/F1.5 (DCS-6112), 0 lux with IR LED (DCS-6113, DCS-6113V) ▪ Built-in Infrared-Cut Removable (ICR) Filter module (DCS-6113, DCS-6113V)
	Image Features	▪ Configurable image size, quality, and bit rate ▪ Time stamp and text overlays ▪ 3 configurable motion detection windows ▪ ePTZ function	▪ 5 configurable privacy masks ▪ Flip & mirror ▪ Configurable white balance, shutter speed, brightness, saturation, contrast, sharpness
	Video Compression	▪ H.264/MPEG4/MJPEG dual format compression simultaneously ▪ JPEG for still image	▪ H.264/MPEG-4 multicast streaming
	Video Resolution	1920x1080@30fps, 1440x1080@30fps, 1280x960@30fps, 1280x720@30fps, 1024x768@30fps, 800x600@30fps, 800x450@30fps, 640x480@30fps, 640x360@30fps, 480x270@30fps, 320x240@30fps, 320x176@30fps	
	Audio Features	▪ G.711 ▪ MPEG-4 AAC	▪ Supports two-way audio and audio mute
Network	Network Protocols	IPv4, IPv6, TCP/IP, UDP, ICMP, DHCP Client, NTP Client (D-Link), DNS Client, DDNS Client (D-Link), SMTP Client, FTP Client, HTTP/HTTPS, Samba Client, PPPoE, UPnP Port Forwarding, RTP/RTSP/RTCP, IP filtering, LLTD, CoS/QoS, SNMP, IGMP, 802.1x	
	Security	▪ Administrator and user group protection ▪ Password authentication ▪ HTTP and RTSP digest encryption	▪ HTTPS streaming ▪ Remote client access control
System Integration	System Requirements	▪ Operating system: Microsoft Windows® 8, 7, or Vista® ▪ Browser: Internet Explorer® 7 or higher	
	D-ViewCam™ System Requirements for Web Interface	▪ Operating System: Microsoft Windows® 8, 7, or Vista® ▪ Web Browser: Internet Explorer® 7 or higher	▪ Protocol: Standard TCP/IP
	Event Management	▪ Motion detection ▪ Tamper Detection ▪ Event notification and upload snapshots/video clips via HTTP, SMTP or FTP	▪ Multiple event notification ▪ Multiple recording methods for easy backup ▪ Supports multiple HTTP, SMTP and FTP servers
	Remote Management	▪ Configuration accessible via web browser ▪ Take snapshots/video clips and save to local hard drive or NAS via web browser	
	Surveillance Software Function	▪ Remote management/control of up to 32 cameras ▪ Viewing of up to 32 cameras on one screen	▪ Supports all management functions provided in web interface ▪ Scheduled motion triggered, or manual recording options
	External Device Interface	▪ DI and DO for external sensor and alarm ▪ External audio input (MIC in) ▪ External audio/video output (AV out)	▪ TV system switch (NTSC/ PAL) ▪ MicroSD card slot

General	Power Input	12 V DC 1.25 A, 50/60 Hz, IEEE 802.3af PoE
	Max. Power Consumption	4.4 W (DCS-6112) 5.3W (DCS-6113, DCS-6113V)
	Operating Temperature	0 to 40 ˚C (32 to 104 ˚F)
	Storage Temperature	-20 to 70 ˚C (-4 to 158 ˚F)
	Humidity	90% non-condensing
	Vandal-proof	IK-10 standard (DCS-6113V)
	Weight	466 g (1.03 lbs) (DCS-6112) 472 g (1.04 lbs) (DCS-6113) 578 g (1.27 lbs) (DCS-6113V)
	Certifications	CE (Class A), CE LVD (EN60965-1), FCC (Class A), ICES-003, C-Tick
Dimensions	DCS-6112, DCS-6113	

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 (e.g. DCS-6112/DCS-6113)
- Hardware Revision (located on the label on the bottom of the camera (e.g. rev A1))
- Serial Number (s/n number located on the label on the bottom of the 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): Five (5) years
- 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 (USA):

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 at https://support.dlink.com, 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 and entering the assigned Case ID Number at http://rma.dlink.com/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Please refer to shipping and packaging instructions located online at http://rma.dlink.com/.

- 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., 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.

Submitting A Claim (Canada):

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:

- Customers need to provide their receipt (proof of purchase) even if the product is registered. Without a receipt, no warranty service will be done. The registration is not considered a proof of purchase.

- 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 at 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 and entering the assigned Case ID Number at https://rma.dlink.ca/.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to 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 be rejected by D-Link. Products shall be fully insured by the customer and shipped 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.

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.

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 Statement:

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 Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and 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 2.0
July 15, 2014