User Manual

HD Wireless IP Camera

Model: FI9851P

Table of Contents

1 Overviews 1
1.1 Key Features 1
1.2 Read Before Use 1
1.3 Packing Contents 2
1.4 Physical Description 2
1.4.1 Front Panel 2
1.4.2 BottomView 3
2 Accessing the Network Camera 4
2.1 Access the Camera in LAN 4
2.2 Access the Camera in WAN 5
2.2.1 Static IP Addresses 5
2.2.2 Dynamic IP Addresses 7
2.3 Using the VLC player 10
3 Surveillance Software GUI 12
3.1 Login Window 13
3.2 Modify the Username and Password 14
3.3 Surveillance Window 15
4 Advanced Camera Settings 20
4.1 Device Status 20
4.1.1 Device Information 20
4.1.2 Device Status 21
4.1.3 Session status 21
4.1.4 Log 21
4.2 Basic Settings 22
4.2.1 Camera Name 22
4.2.2 Camera Time 22
4.2.3 User Accounts 23
4.2.4 Multi-Camera 26
4.3 Network 30
4.3.1 IP Configuration 31
4.3.2 Wireless Settings 32
4.3.3 PPPoE 34
4.3.4 DDNS 35
4.3.5 UPnP 38
4.3.6 Port 39
4.3.7 Mail Settings 44
4.3.8 FTP Settings 46
4.3.9 P2P 47
4.4 Video 48
4.4.1 Video Settings 48
4.4.2 On Screen Display 49
4.4.3 Privacy Zone 49

4.4.4 Snapshot Settings....51
4.4.5 IR LED Schedule....51
4.4.6 Lens Distortion Correction....52
4.5 Alarm....52
Motion Detection....52
4.6 Record....56
4.6.1 Storage Location....56
4.6.2 Local Alarm Recording....56
4.6.3 Schedule Recording....56
4.7 Firewall....57
4.8 System....58
4.8.1 Back-up& Restore....58
4.8.2 System Upgrade....58
4.8.3 Factory Reset....60
4.8.4 Reboot....60
5 Appendix....60
5.1 Frequently Asked Questions....60
5.1.1 Install / uninstall the ActiveX of Firefox browser....60
5.1.2 Install / uninstall the ActiveX of Google Chrome....65
5.1.3 Install / Uninstall the ActiveX of IE Browser....68
5.1.4 I have forgotten the administrator password....72
5.1.5 Camera can not record....72
5.1.6 Subnet doesn't match....73
5.1.7 No Pictures Problems....73
5.1.8 Can't access IP camera in internet....74
5.1.9 UPnP always failed....74
5.1.10 Camera can not connect wireless....74
5.1.11 Can't see other cameras listed in multi-device when using remote access....74
5.2 Default Parameters....74
5.3 Specification....75
5.4 CE & FCC....76
5.5 Warranty....77
6 Obtaining Technical Support....79

1 Overviews

FI9851P is integrated IP Camera with a color CMOS sensor enabling viewing resolution 1280*720. It combines a high quality digital video camera, with a powerful web server, to bring clear video to your desktop from anywhere on your local network or over the Internet.

They support the industry-standard H.264 compression technology, drastically reducing file sizes and conserving valuable network bandwidth.

The IPCAM is based on the TCP/IP standard. There is a WEB server inside which could support Internet Explorer. Therefore the management and maintenance of your device is simplified by using the network to achieve the remote configuration and start-up.

The camera is designed for outdoor and indoor surveillance applications such as courtyards, supermarket, and school. Controlling the IPCAM and managing images are simplified by using the provided web interface across the network utilizing wireless connectivity.

FOSCAM provides Phone Apps for Android and iPhone users, please search **Foscam Viewer** and install it through APP Store, then you can view your camera directly as a computer.

1.1 Key Features

- Standard H.264 video compression algorithm to satisfy the transmission of high definition video in narrow bandwidth network
- 1.0 Mega-Pixel
- Supports IE/Firefox/Google/Safari browser or any other standard browsers
- Supports WEP, PA and WPA2 Encryption
- IR night vision , Range:10m
- Supports image snapshot
- Supports dual-stream
- Supports IR-Cut and the filter change automatically
- Embedded FOSCAM DDNS(dynamic domain name service) Service
- Supports remote viewing & record from anywhere anytime
- Multi-level users management with password protection
- Motion detection alert via email or upload image to FTP
- Supporting Third Party Domain name
- Providing Phone APPs for Android and iPhone users
- Supports multiple network protocols: HTTP/HTTPS/RTSP/TCP/IP/UDP/FTP/DHCP/DDNS/UPNP/ONVIF
- Providing Central Management Software to manage or monitor multi-camera

1.2 Read Before Use

Please first verify that all contents received are complete according to the Package Contents listed below.

Before the Network Camera is installed, please carefully read and follow the instructions in the Quick Installation Guide to avoid damage due to faulty assembly and installation. This also ensures the product is used properly as intended.

1.3 Packing Contents

● IPCAM×1	● CD×1
● DC Power Supply×1	● Quick Installation Guide ×1
● Network Cable×1	● Warranty Card×1

1.4 Physical Description

1.4.1 Front Panel

Figure 1.1

1 Infrared Lamp
2 LENS: CMOS sensor with fixed focus lens
3 Induction IC

1.4.2 BottomView

There are two labels located at the bottom of the camera; this is an important feature of original Foscam cameras. If your camera does not have labels as shown in Figure 1.3, it may be a clone. Cloned Foscam cameras can not use original firmware and are not eligible for warranty or technical services.

2 Accessing the Network Camera

This chapter explains how to access the network camera through web browsers and RTSP players.

2.1 Access the Camera in LAN

This camera support HTTP and HTTPS protocols, so here will allow you to use HTTP and HTTPS port No.

(1) Http:// LAN IP + Http Port No.

Double click the IP Camera Tool icon and it should find the camera's IP address automatically after you plug in the network cable.

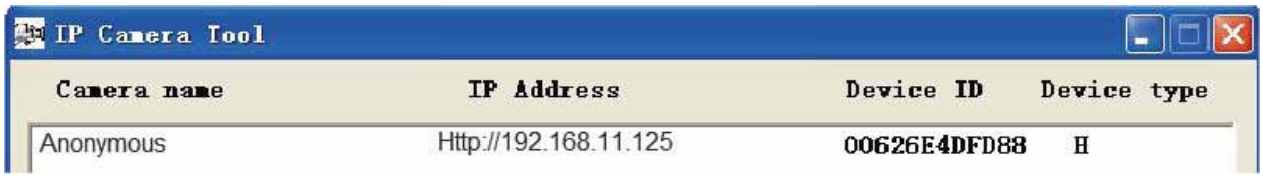


Figure 2.1

Double click the IP address of the camera; your default browser will open to the camera login page.

(2) Https:// LAN IP + Https Port NO.

The default Https port no. is 443. You can use the url to access the camera: **https:// LAN IP + HTTPS port**. Go to **Settings - Network - Port** panel , you can see and change the https port NO.

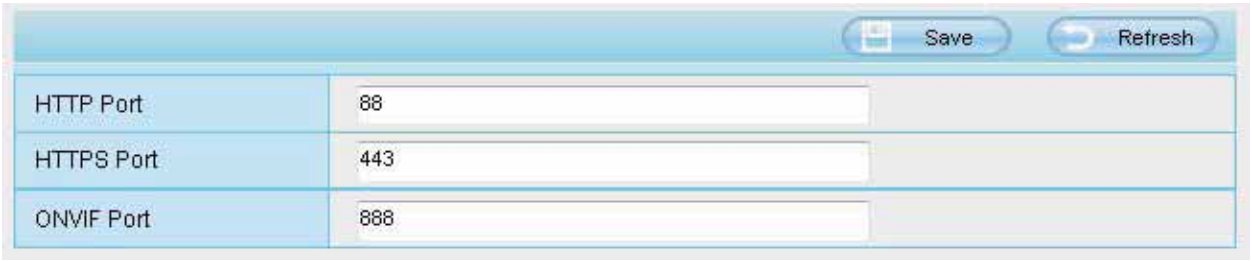


Figure 2.2

2.2 Access the Camera in WAN

2.2.1 Static IP Addresses

Users who have static IP addresses do not need to set DDNS service settings for remote access. When you have finished connecting the camera using the LAN IP address and port forwarding, you can access the camera directly from the Internet using the WAN IP address and port number.

How to Obtain the WAN IP address from a public website ?

To obtain your WAN IP address, enter the following URL in your browser: http://www.whatismyip.com.The webpage at this address will show you the current WAN IP.

Figure 2.3

Access your IP Camera from the Internet

You can access the IP Camera from the Internet (remote access). Enter the WAN IP address and port number in your standard browser. For example, you would enter http:// 183.37.28.254:85

NOTE :
Make sure port forwarding is successful. You can do port forwarding two ways.

1. Login to your router to enable the “UPNP” function. You can then login to the camera as administrator, choose Network, and then choose UPnP to enable UPnP. Make sure that the status of UPnP reads “UPnP Successful” on the Device Status page.
2. Do port (HTTP port) forwarding manually. (See Figure 2.11 for further details)
If your router has a Virtual Server, it can do port forwarding. Add the camera’s LAN IP and port which you had set earlier to your router’s port forwarding settings.

NOTE: If you plug the camera into a router, it will have a dynamic IP address and you need to set DDNS service settings to view it remotely.

Step 1: Enter the username and password of the Administrator (default username is admin with a blank password), and click “OK” to apply changes.
Step 2: Wait around 10 seconds, you’ll see that the camera’s LAN IP address has changed. In our example it was changed to 2000, so we see http://192.168.8.102:2000 in IP Camera Tool. Also, the LAN IP address is now fixed at a static IP address of http://192.168.8.102:2000. This IP address will not change even if the camera is powered off and back on, the camera will remain on this LAN IP address. This is very important that a static LAN IP address is set, or you may have problems later with remote access and seeing the camera remotely if the camera loses power and reconnects on a different LAN IP address. Make sure you set a static LAN IP address!

2.2.2 Dynamic IP Addresses

DDNS is a service that allows your IP Camera, especially when assigned with a dynamic IP address, to have a fixed host and domain name. This means that even though your WAN IP address is constantly changing, you will have a fixed hostname you can use to access your cameras at all times. You can access the camera directly from the Internet using the hostname and port number.

What is the HTTP Port NO.?

1) Default HTTP Port is 88

All cameras have the default HTTP port of 88. For example, if the LAN IP link of the camera is http://192.168.8.102:88, this means that the camera’s HTTP port is 88. You can change port 88 to another port if you’d like such as 2000 or 8090, which will not be conflict with other existing ports like 25, 21,10000.Here you can set the port no. between 1 and 65535.

2) Change the default http no.88 to another one.

How to assign a different HTTP Port No. and fixed the LAN IP of the camera by the IP Camera Tool？
Step 1: Open the IP Camera Tool, select the camera you would like to change the port of, right click on the IP address, and click on ”Network Configuration”, this brings up the network configuration box as shown in Figure

2.4 and 2.5.

Figure 2.4

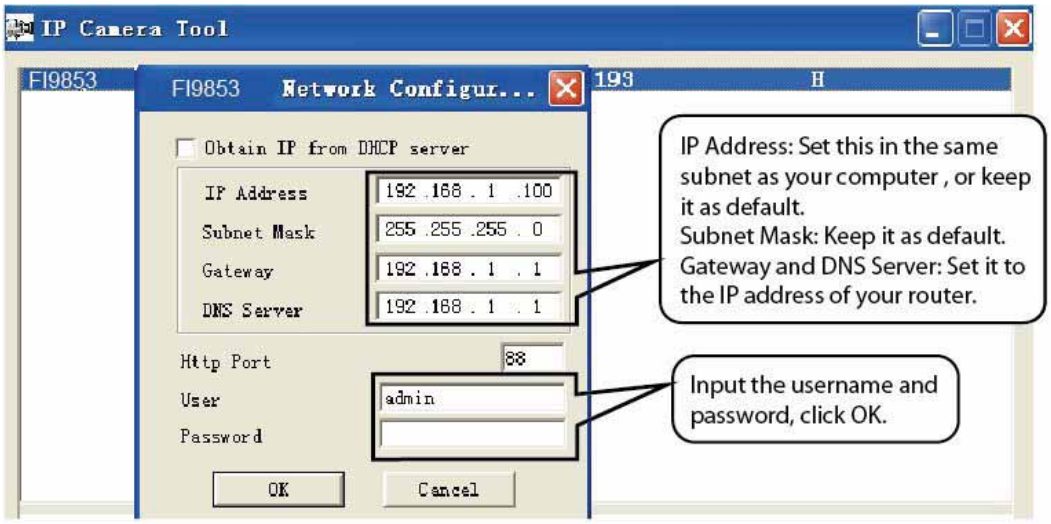


Figure 2.5

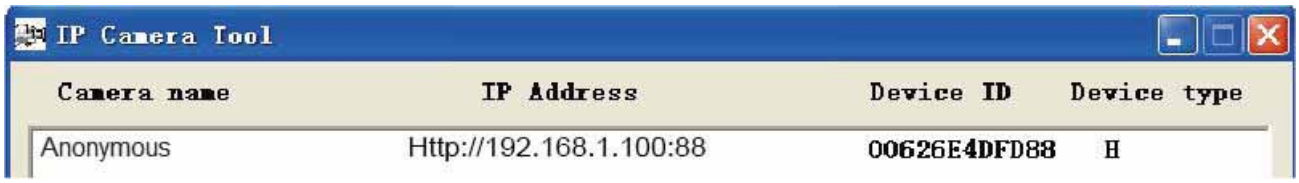


Figure 2.6

What is Port forwarding ?

If you have never done port forwarding before, you can open and view the following link to understand the basic concept. Port forwarding allows for outside connections to access a specific device on your network from anywhere in the world. Every router automatically blocks any incoming connections for safety purposes. Using port forwarding, you are telling your router to allow a connection through a certain port (you can think of it as a gateway) into your router. You set this port to a specific device, in our case an IP Camera, so it can be accessed from anywhere in the world.

Click this link to learn more about port forwarding: http://portforward.com/help/portforwarding.htm

How do we configure Port Forwarding ?

For this section, we will be using an example:

Let's say the camera's LAN IP address is http://192.168.8.100:2000

Step 1: Login to the router, and go to your router's port forwarding or port triggering menu. Sometimes this is also under the name of Virtual Server or NAT.
Using the Linksys brand router as an example, we would log into the router, and go to the Applications & Gaming menu. We would then click on the "Single Port Forwarding" sub-menu.

Step 2: Create a new column using the LAN IP address & HTTP Port of the camera within the router as shown below, then push OK or Submit to save your settings:

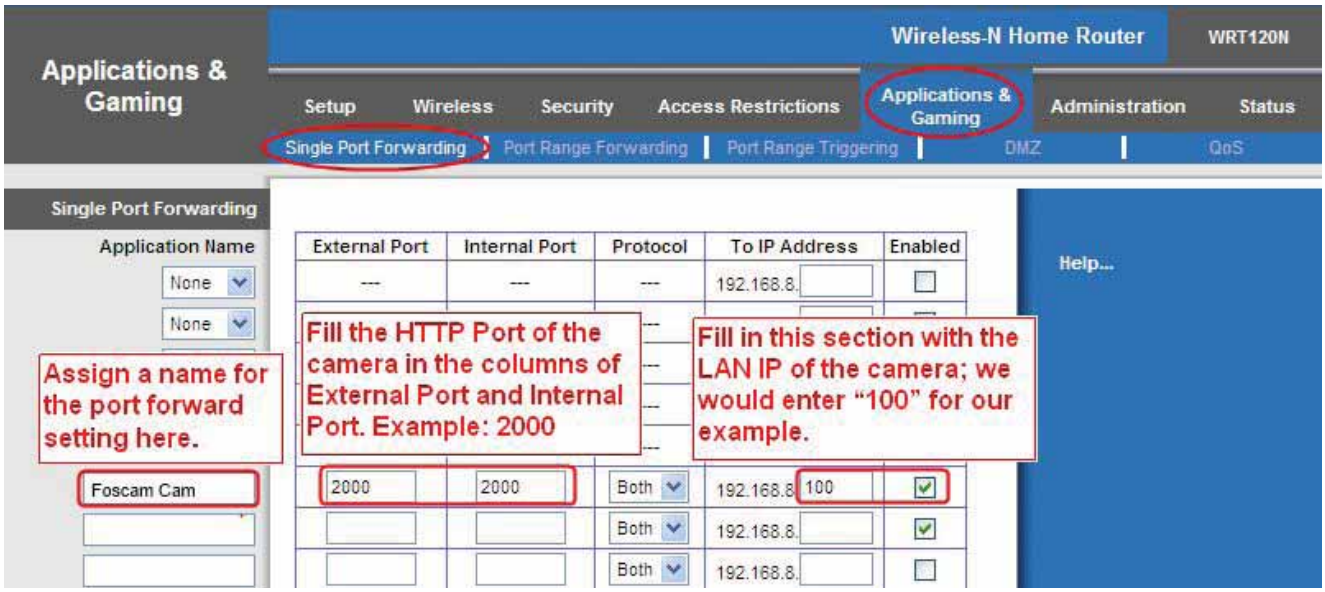


Figure 2.12

First method :

Use the embedded DDNS to access the camera via the Internet

Each Foscam camera has an embedded unique DDNS domain name, the format of this domain name is xxxxxx.myfoscam.org. On the bottom of the camera, you can see the domain name sticker with this information on it.

For example, we can use **cp4911.myfoscam.org**. In the camera, click Settings at the top, click "Network" on the left, then click "DDNS" to get to the DDNS settings page. Here you can see the unique domain name of your camera.

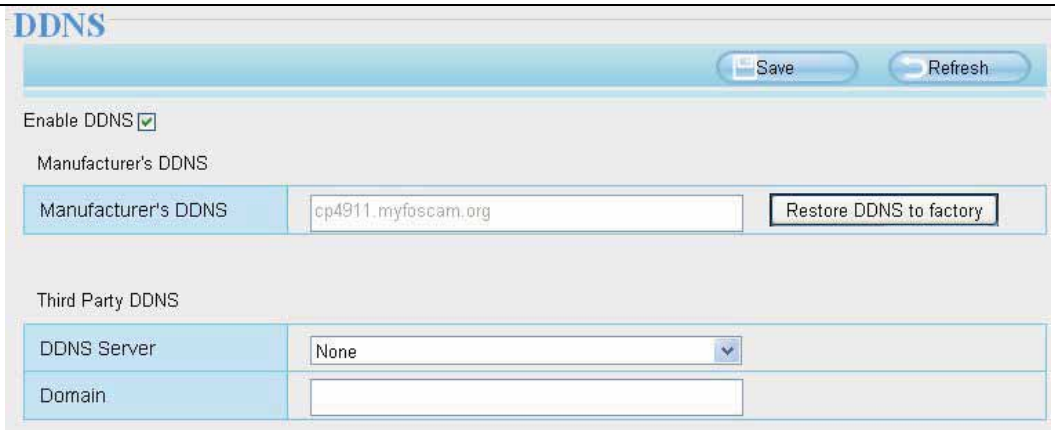


Figure 2.13

Now you can use "http://Domain name + HTTP Port" to access the camera via the Internet.
Take hostname cp4911.myfoscam.org and HTTP Port of 2000 for example, the URL link to access the camera via the Internet would be http:// test09.myfoscam.org:2000.

Second method :
Use the Third party DDNS to access the camera via the Internet

Step 1, Please go to the third party DDNS website(such as www.no-ip.com) to create a free hostname.
Step 2, DO DDNS Service Settings within the Camera

Please set DDNS Settings within the camera by **hostname**, a user name and password you've got from **www.no-ip.com**
Take hostname ycxgwp.no-ip.info, user name **foscam**, password **foscam2012** for example.

Firstly, goes to option of DDNS Settings on the administrator panel.
Secondly, select No-Ip as a server.
Thirdly, fill foscam as DDNS user, fill password **foscam2012** as DDNS password, fill ycxgwp.no-ip.info as DDNS domain and server URL, Then click save to make effect. The camera will restart and to take the DDNS settings effective.
Fourthly, after the restart, login the camera, and go to option of Device Status on the administrator panel, and check if the DDNS status is successful.
If failed, please double check if you have input the correct hostname, user name, and password, and try to redo the settings.

NOTE :
If you have set Third Party DDNS successfully ,the Foscam Domain Name will be invalid. The Third Party DDNS and the Foscam Domain Name cannot work at the same time, the last time you configured will take effect.

2.3 Using the VLC player

This camera supports RTSP streaming, here you can view the camera using VLC player.

RTSP URL rtsp:// [user name][:password]@IP:HTTP port number/videosream

The part in the square brackets may be omitted.

user name & password:

The user name and password to access the camera. This part can be omitted.

IP: WAN or LAN IP address.

Videostream: Here support three modes: videoMain, videoSub and audio. When the network speed is bad, here you had better select videoSub. If you select audio, you can only hear the sound but cannot see the video.

For example:

IP: 192.168.1.11

HTTP Port number: 88

User name: admin

Password: 123

Here I can enter one of the following URLs in the VLC.

1. rtsp://admin:123@192.168.1.11:88/videoMain
2. rtsp:// @192.168.1.11:88/videoMain
3. rtsp://:123@192.168.1.11:88/videoMain
4. rtsp://admin@192.168.1.11:88/videoMain

Open the VLC, and go to Media(Open Network Stream option, then enter the URL into VLC.

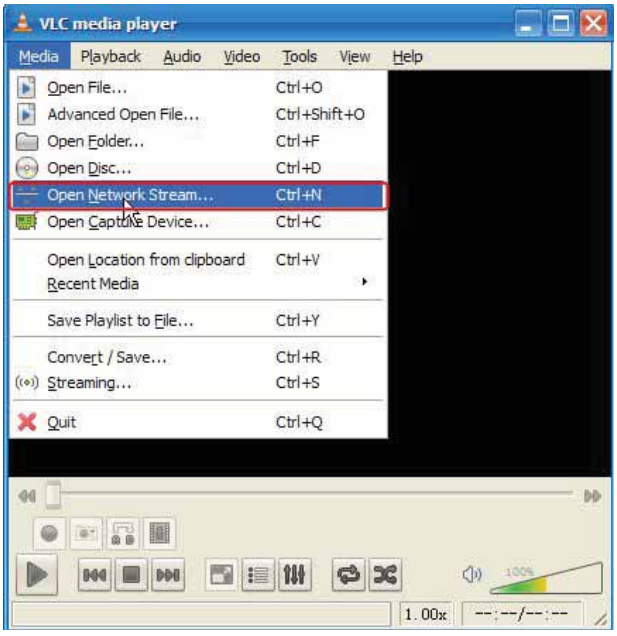


Figure 2.14

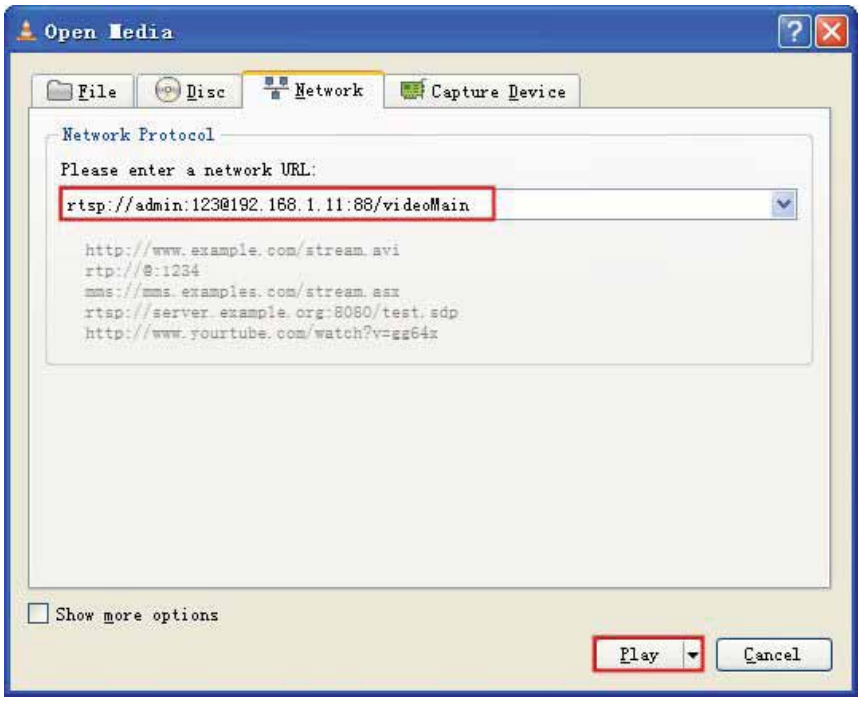


Figure 2.15

Sometimes you may need to enter the user name and password again. Click OK and you can see the real-time preview.

Figure 2.16

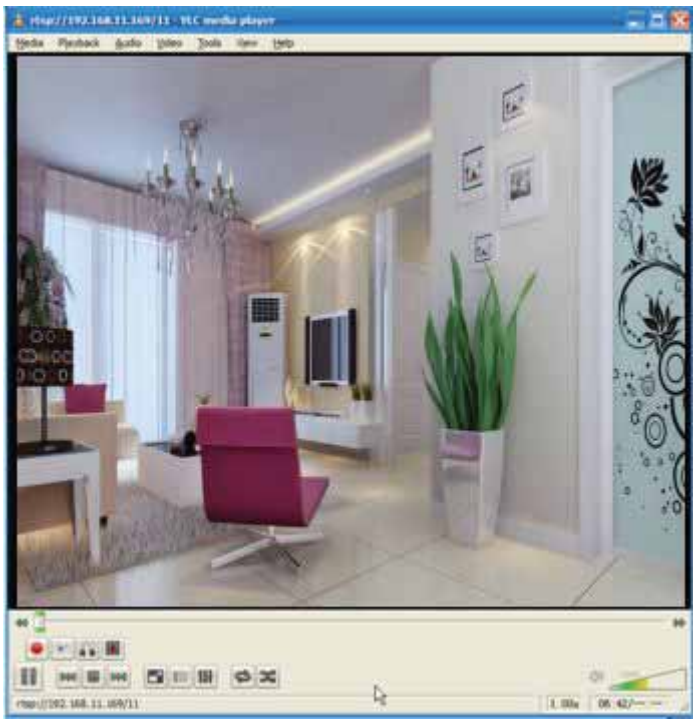


Figure 2.17

If you cannot play the video in the VLC player, please check the port mapping. You can read Quick Installation Guide about How to configure port forwarding.

NOTE:
If you modify the camera's username or password, you had better reboot the camera, or else the new username and password cannot take effect when you enter the authentication in the VLC.

3 Surveillance Software GUI

Please refer to the Quick Installation Guide if you install the camera at first time. After finishing quick installation, you can take time to learn the operation of the software.

3.1 Login Window

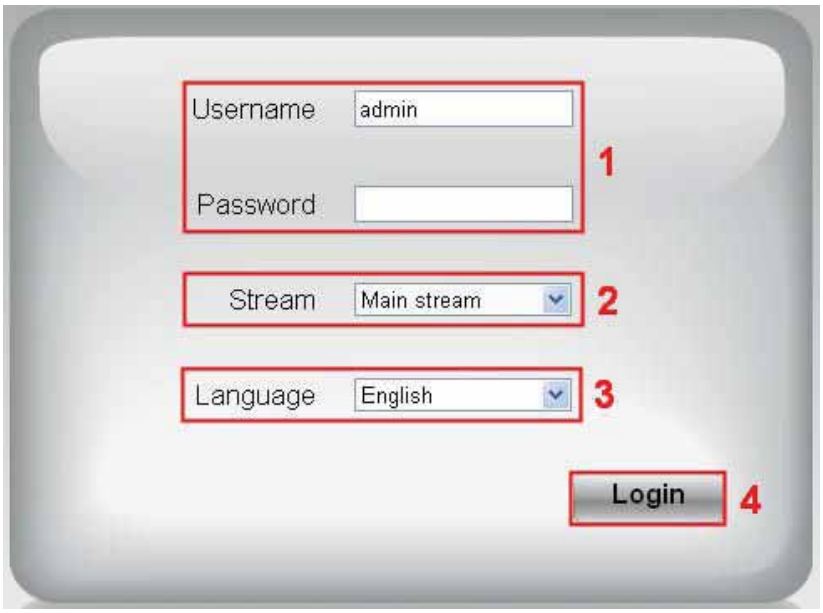


Figure 3.1

Please check the login window above, it was divided to 4 sections from no. 1 to 4.

Section1 Enter the Username and password

The default administrator username is admin with no password, please reset the password at first using and prevent unauthorized users login the camera (read chapter 3.2.4 about how to change).

Section2 Stream

The camera supports two stream modes: Main stream and sub stream. If you want to access the camera form LAN, here you can select Main stream. If you want to access the camera from Internet, here we recommend sub stream.

NOTE: When the network bandwidth is badly you'd better select Sub Stream and the video will be more fluency.

Section3 Select the language

You can select the language you need via click on the language dropdown list to switch.

Section4 Login the camera

Click Login button and you will see the surveillance windows.

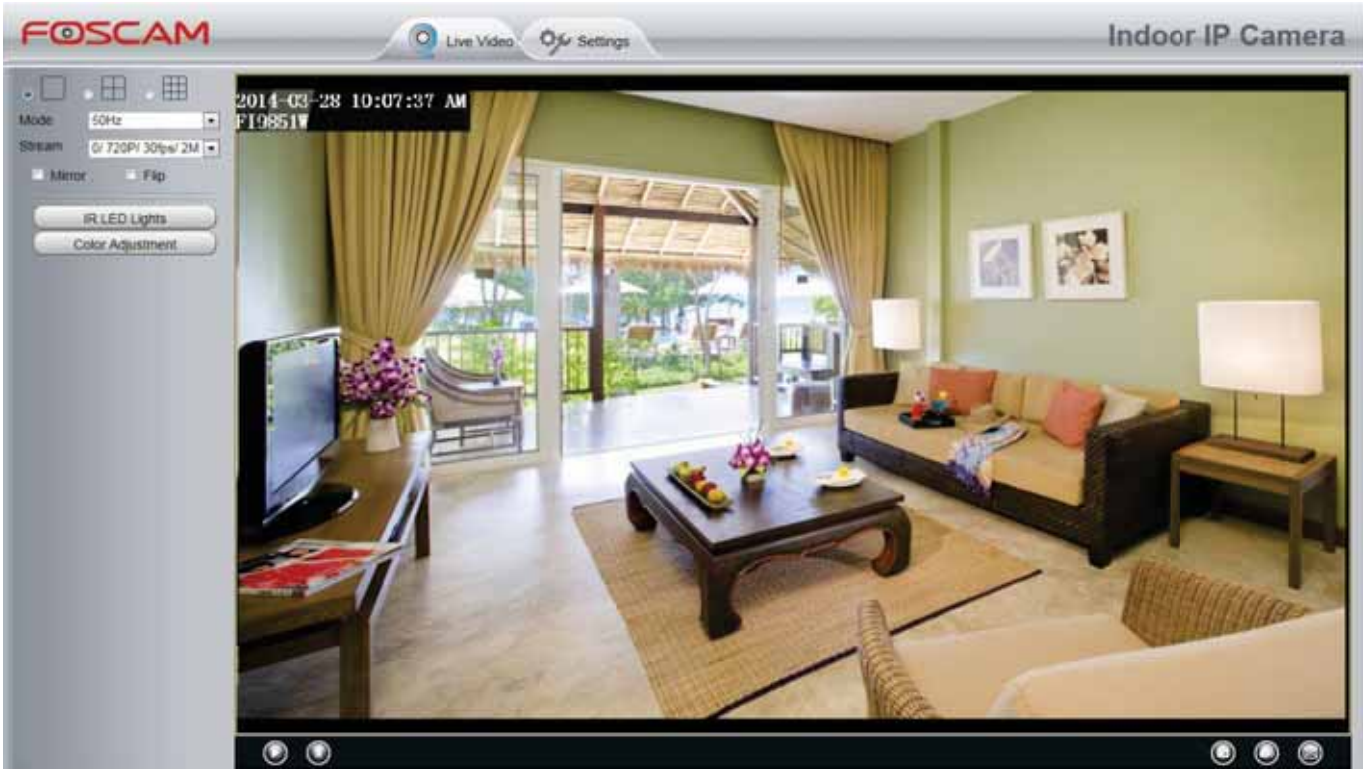


Figure 3.2

3.2 Modify the Username and Password

When you log in for the first time, it will come to the operating of modify the username and password automatically.

Figure 3.2

Enter the New Username, New password and Confirm the password.
Click **Modify** button, you will see the login page again.

3.3 Surveillance Window

Figure 3.3

Section1 FOSCAM Logo/ LiveVideo / Settings buttons

: FOSCAM LOGO

: Path to surveillance window. Click this button and back to the surveillance window

: Path to Administrator Control Panel, Click it, and it will lead to Administrator Control Panel and do advanced settings.

Section2 Multi-Device Window

The firmware inside the camera supports up to maximum of 9 cameras being monitoring at the same time. You can add other cameras in multi-camera panel (read chapter 4.2.5).

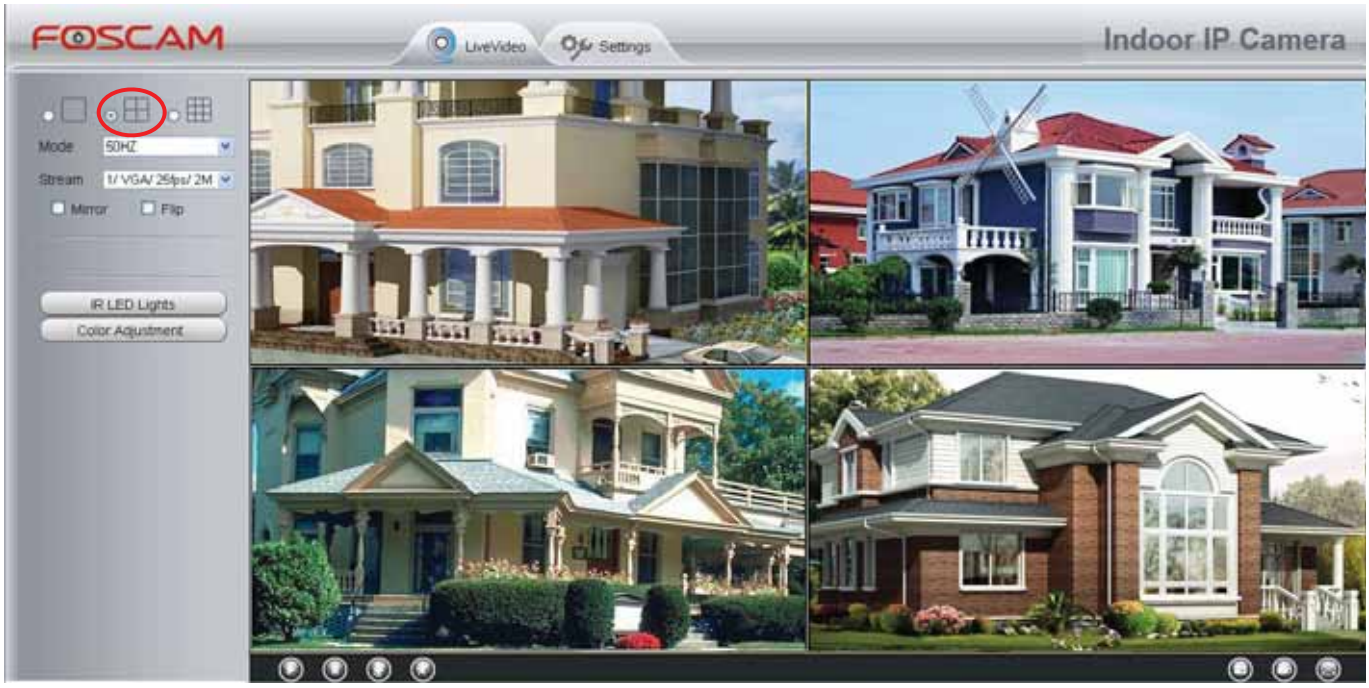


Figure 3.4

Section3 Mode/ Stream / Mirror/ Flip buttons

Mode

1) 50Hz ---------Indoor surveillance (Region: Europe, China)

2) 60Hz ---------Indoor surveillance (Region: USA, Canada)

3) Outdoor Mode------Outdoor surveillance

Stream

The default Stream supports four modes:

0/720P/30fps/2M, 1/VGA/25fps/4M, 2/VGA/15fps/1M and 3/VGA/10fps/200K

The format of the stream type is **Stream type no. / Resolution / Maximum frame rate/ Bit rate**

1) Stream type no. : The number is used to identify the stream type.

2) 720P/ VGA

There are two resolutions, the bigger one is 720P, and the smaller one (VGA) is 640x480 pixels. The bigger the resolution, the better of the image quality is. If you are accessing the camera via internet and want to get more fluent video streaming, please select resolution VGA.

3) Maximum frame rate

When the video format is 50Hz, the maximum frame rate is 25 fps. When the video format is 60Hz, the maximum frame rate is 30 fps. You should lower frame rate when the bandwidth is limited. Normally, when the frame rate above 15, you can achieve fluently video.

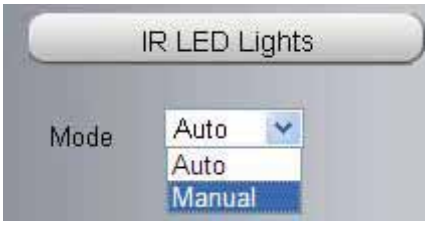
4) Bit rate

Generally speaking, the larger the bit rate is, the clearer video will become. But the bit rate configuration should combine well with the network bandwidth. When the bandwidth is very narrow, and bit rate is large, that will lead to video cannot play well.

You can reset the stream type on Settings-> Video-> Settings panel(chapter 4.4.1).

After changing, please re-login the camera and you can see the modification.

Section4 IR LED Lights



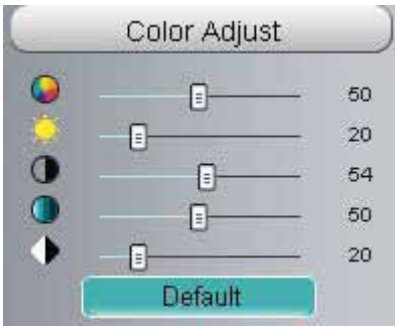
Click IR LED Lights and there are two modes to adjust the infrared led: Auto and Off . The default mode is Auto.

Auto: Select it and the camera will adjust the infra led (on or off) automatically.

Manual: Select it and turn off the infra led manually.

Section5 Image quality settings

In this page, you can tune Hue, Brightness, Contrast, Saturation, and Sharpness to get higher quality.



Section6 OSD

If you have added time and camera name in the video, you can see it in the live window.

Go to **Settings ---Basic settings---Camera name** panel, and you can change another device name. The default device name is anonymous.

Go to **Settings ---Basic settings---Camera time** panel and adjust the device time.

Go to **Settings ---Video---On Screen Display** panel, you can add or no add OSD.

Section7 Play/Stop/ Talk/Audio/ Snap/ Record/ Full screen button

1------Play Click it to play the video of the camera

2------Stop Click it to stop the video of the camera

3------ Talk: Click the button and the icon will become to , then talk to the microphone that connected with PC, people around the camera can hear your voice if the camera has connected with audio output device.

Click the icon again and stop talking.

4------ Audio Click the button and the icon will become to , you can hear the sound around the camera if the camera has connected with other audio input device through the Audio Input port of the camera, Click the icon again and stop audio.

5----- Snap: Click it to make snapshot and it pop up a window which picture you snapshot, right click in the window and save the picture to anywhere you want.

6----- Record: Click the icon and the camera start recording, you can see a green dot in the live window. Click again and stop recording. The default storage path is C:\IPCamRecord. You can change the storage path: Go to Settings- >Record-> Storage Location panel.

7------Full Screen Click it to make full-screen, or you can double click the surveillance screen to make full-screen. Double click again and exit full-screen.

Onscreen Mouse Control

Right click the mouse and you can adjust the screen ration, full screen and Zoom up.

Figure 3.5

Keep ration: Select it and the camera will adjust the size of live window based on the computer monitor automatically.

Sometimes there is a black border around the video (Figure 3.7), please select Keep ration to get a better visual quality (Figure3.3).

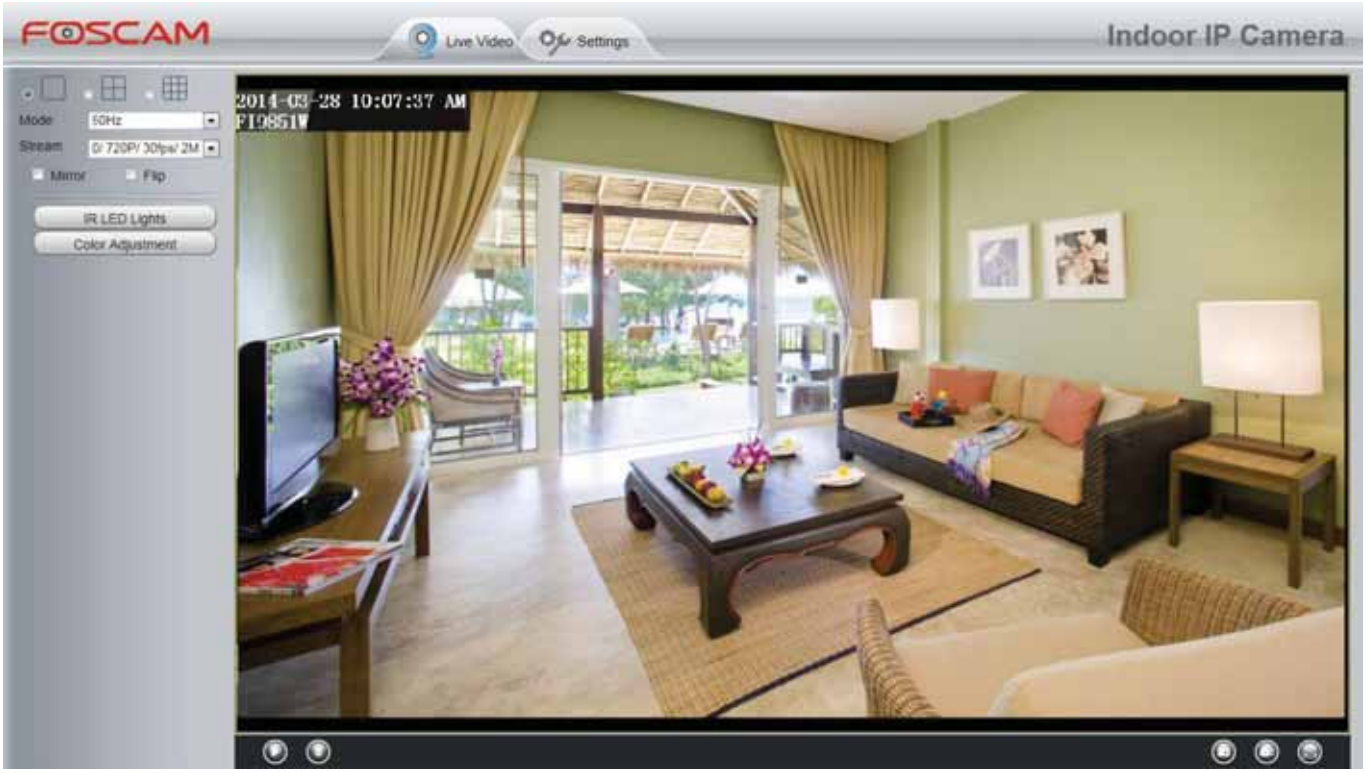


Figure 3.6

Full Screen: Select it and Click it to make full-screen, press ESC and exit full-screen.
Zoom up/down: Click it and the live view will be digital zoomed up, then click Zoom Down and the live view back to original size.

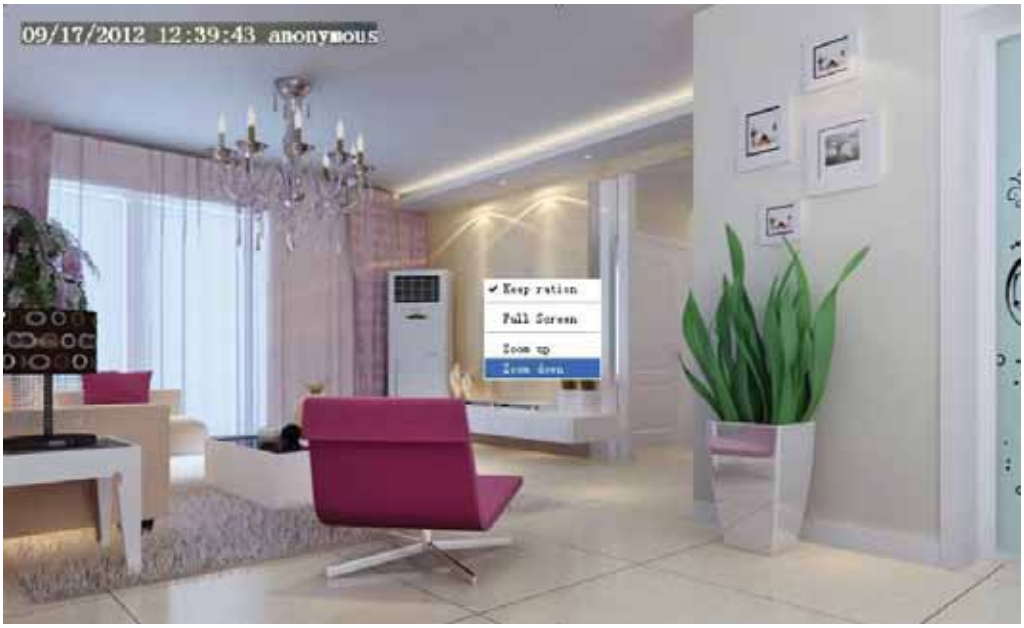


Figure 3.7

NOTE:
For Mac OS, the plugin cannot support Onscreen Mouse function, so you cannot allow to use it.

4 Advanced Camera Settings

Click the button “Settings”, goes to Administrator Control Panel to make advanced camera settings.

4.1 Device Status

Device Status contains four columns: Device Information, Device Status, Session Status and Log, it will show you various information about your camera.

4.1.1 Device Information

Figure 4.1

Camera Model: The model of the device.

Camera Name: The Device Name is a unique name that you can give to your device to help you identify it. Click Basic Settings and go to Device Name panel where you can change your camera name. The default device name is anonymous.

Camera ID: Display the MAC address of your camera. For example Device ID is 008414350787, the same MAC ID sticker is found at the bottom of the camera.

Camera Time: The system time of the device. Click Basic Settings and go to Camera Time panel and adjust the time.

System Firmware version: Display the System Firmware version of your camera.

App Firmware version: Display the application firmware version of your camera.

Plug-in version: Display the plug-in version of your camera

4.1.2 Device Status

On this page you can see device status such as Alarm status, NTP/DDNS status and so on.

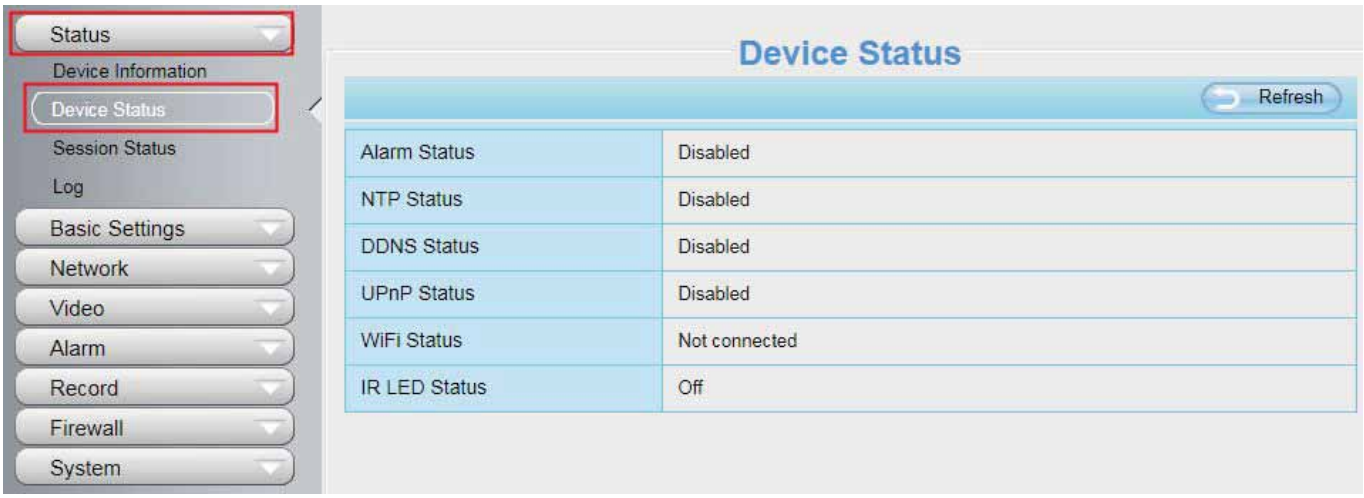


Figure 4.2

4.1.3 Session status

Session status will display who and which IP is visiting the camera now.

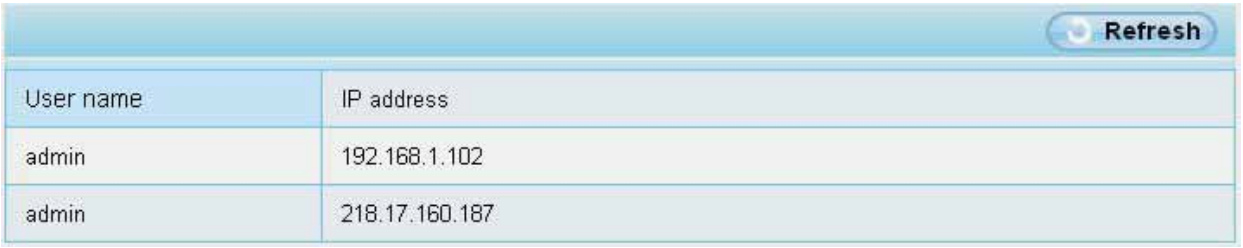
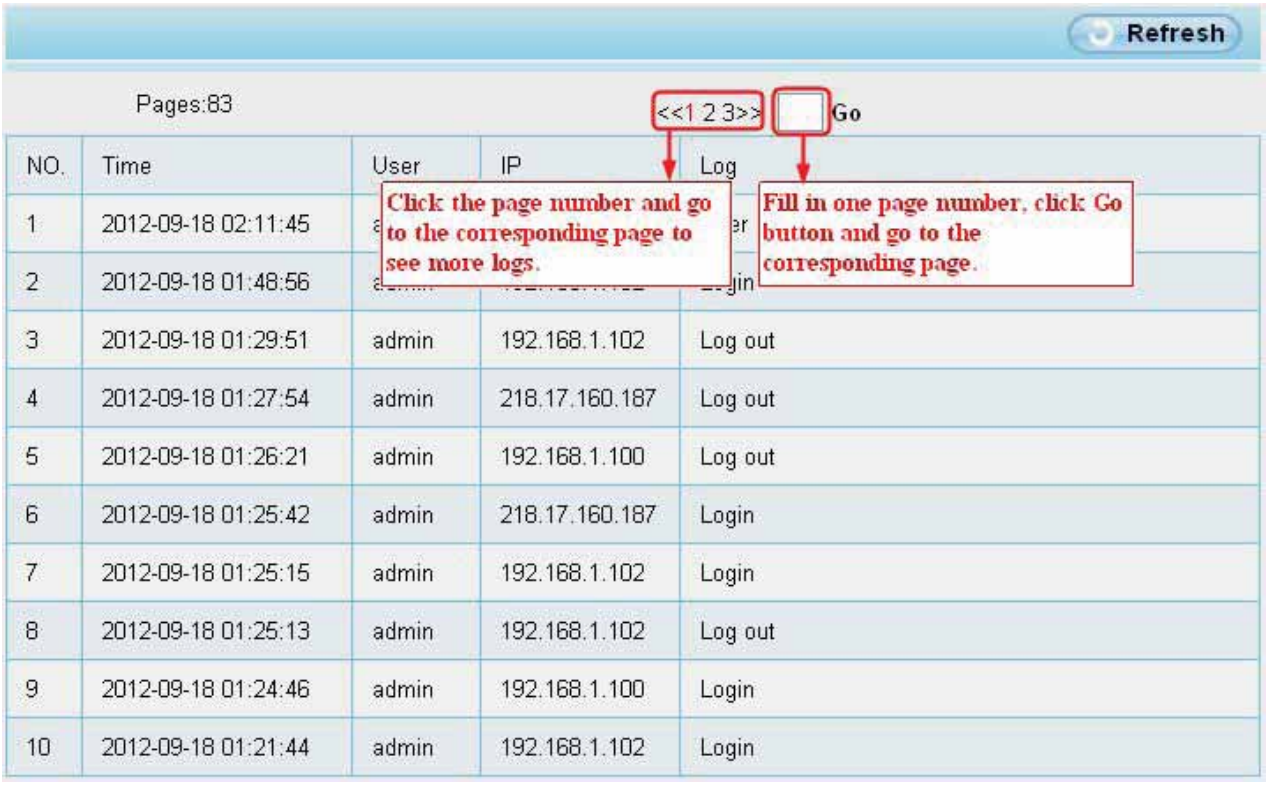


Figure 4.3

4.1.4 Log

The log record shows who and which IP address accessed or logout the camera.



NO.	Time	User	IP	Log
1	2012-09-18 02:11:45			
2	2012-09-18 01:48:56			
3	2012-09-18 01:29:51	admin	192.168.1.102	Log out
4	2012-09-18 01:27:54	admin	218.17.160.187	Log out
5	2012-09-18 01:26:21	admin	192.168.1.100	Log out
6	2012-09-18 01:25:42	admin	218.17.160.187	Login
7	2012-09-18 01:25:15	admin	192.168.1.102	Login
8	2012-09-18 01:25:13	admin	192.168.1.102	Log out
9	2012-09-18 01:24:46	admin	192.168.1.100	Login
10	2012-09-18 01:21:44	admin	192.168.1.102	Login

Figure 4.4

4.2 Basic Settings

This section allows you to configure your Camera Name, Camera Time, Mail, User Accounts and Multi-Device.

4.2.1 Camera Name

Default alias is anonymous. You can define a name for your camera here such as apple. Click **Save** to save your changes. The alias name cannot contain special characters.

Figure 4.5

4.2.2 Camera Time

This section allows you to configure the settings of the internal system clocks for your camera.

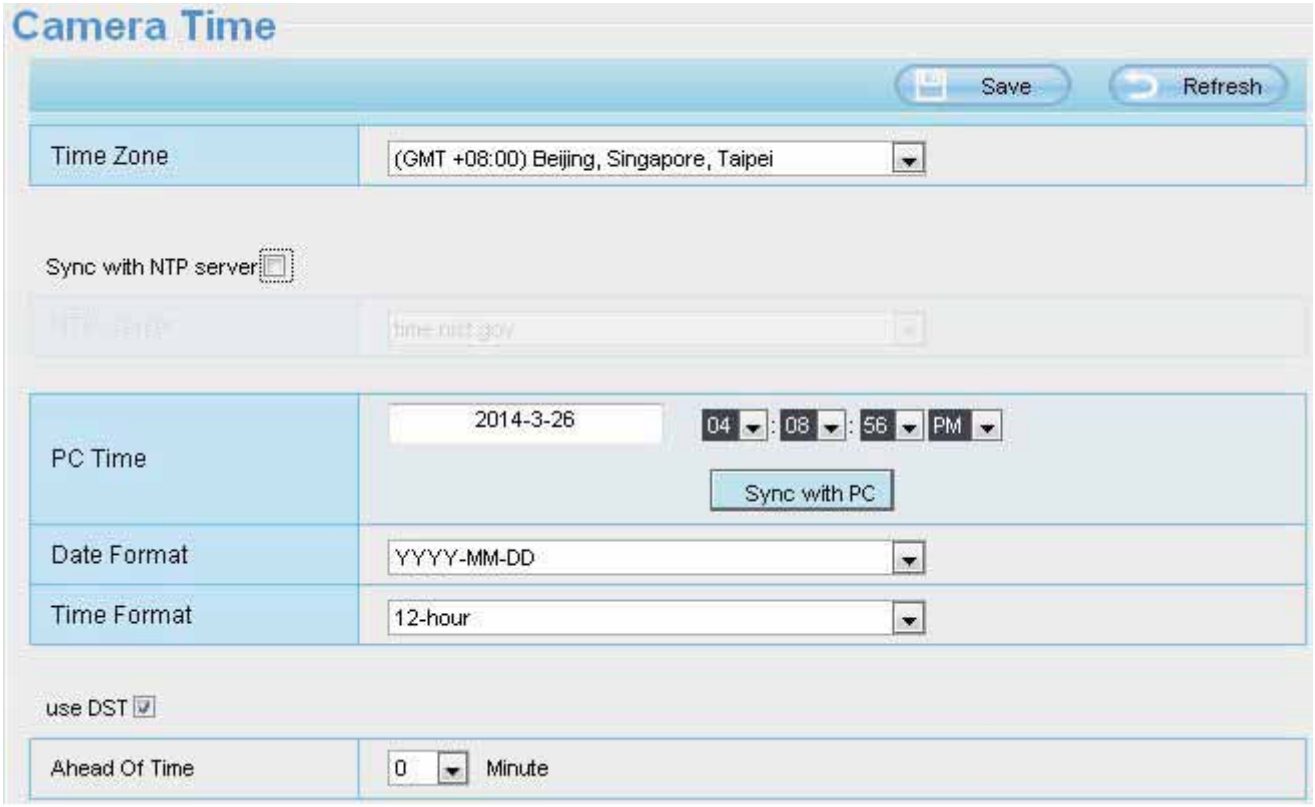


Figure 4.6

Time Zone: Select the time zone for your region from the dropdown menu.
Sync with NTP server: Network Time Protocol will synchronize your camera with an Internet time server. Choose the one that is closest to your camera.
Sync with PC: Select this option to synchronize the date and time of the Network Camera with your computer.
Manually: The administrator can enter the date and time manually. Note select the date and time format.
use DST: Select the daylight saving time from the dropdown list.

Click **Save** button and submit your settings.

4.2.3 User Accounts

Here you can create users and set privilege, **visitor**, **operator or administrator**. The default administrator user accounts are admin with a blank password.

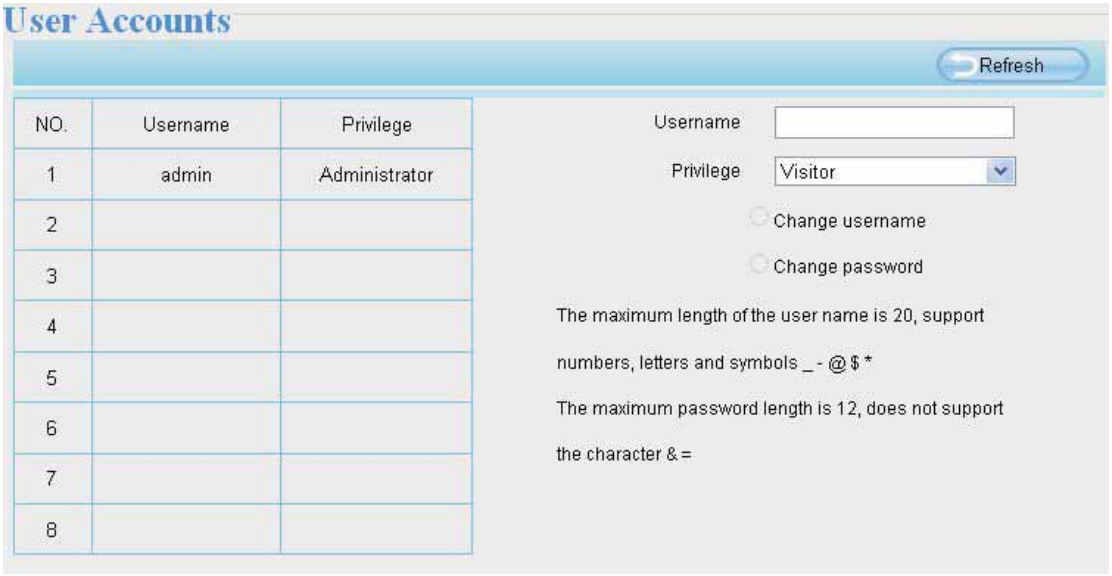


Figure 4.7

How to change the password?

Firstly, select the account which you want to change the password, then select “Change password”, enter the old password and the new password, lastly click modify to take effect.

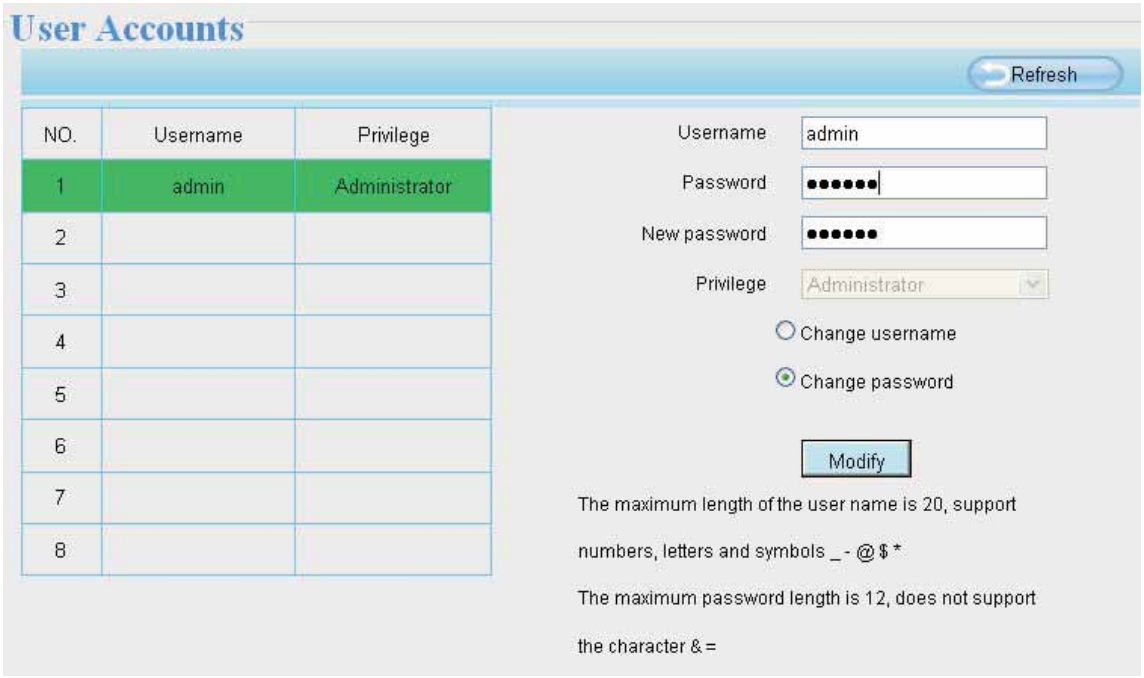


Figure 4.8

How to add account ?

Select one blank column, then enter the new user name, password and privilege, last click Add to take effect. You can see the new added account on the Account list.

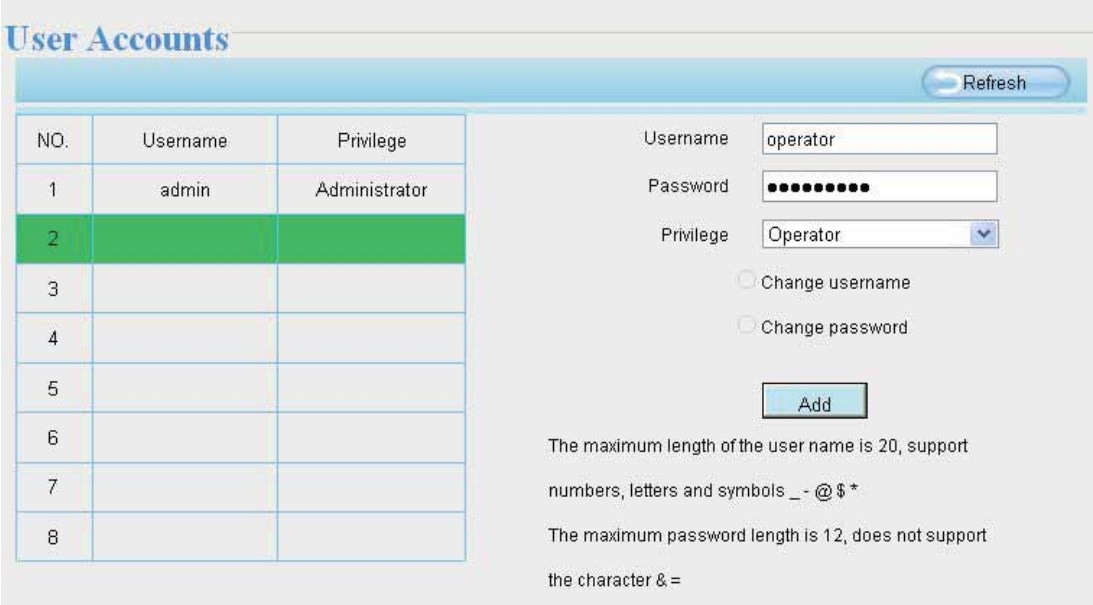


Figure 4.9

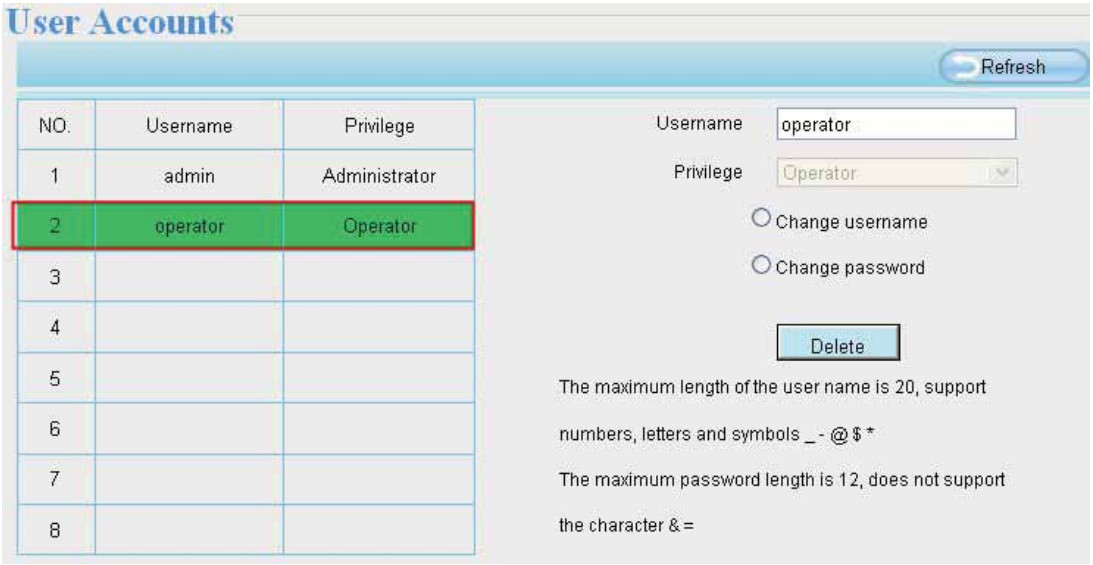


Figure 4.10

Delete : Select the account which you want to delete, then click Delete button to take effect.

NOTE: The default administrator account cannot be deleted, but you can add other administrator users.

How to change the username ?

Firstly, select the account which you want to change the username, then select “Change username”, enter the new password, lastly click modify to take effect.

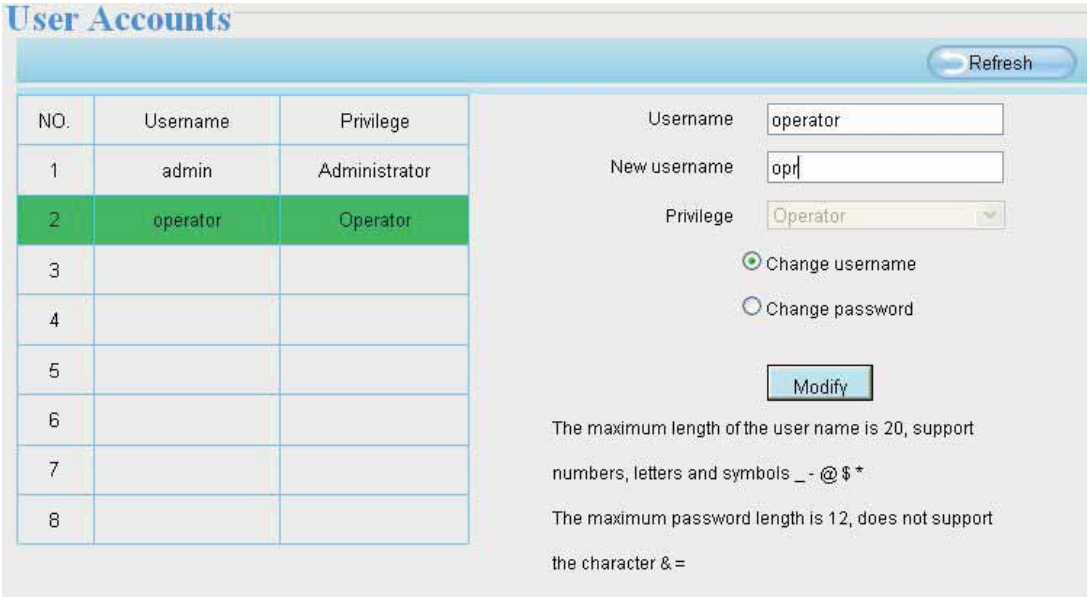


Figure 4.11

4.2.4 Multi-Camera

If you want to view multi-surveillance screens on one window, you need to login one camera, and set it as the main device, and do Multi-Device Settings, add other cameras to the first one camera. Before you do multi-cams settings, you need to assign different port such as 81, 82, 83, 84, 85, 86, 87, 88 to the cameras if there is 8 cams installed.

The firmware within the camera can support a maximum of 9 devices monitoring all at the same time. This page you can both add FOSCAM MJPEG and H.264 series cameras to the first camera and view multi-surveillance screen on one window.

Add cameras in LAN

In Multi-Device Settings page, you can see all devices searched in LAN. The 1st Device is the default one. You can add more cameras in the list in LAN for monitoring. The camera's software supports up to 9 IP Cameras online simultaneously. Click The **2nd Device** and click the item in the Device List in LAN, the Alias, Host and Http Port will be filled in the boxes below automatically. Enter the correct username and password then click **Add**. Add more cameras in the same way.

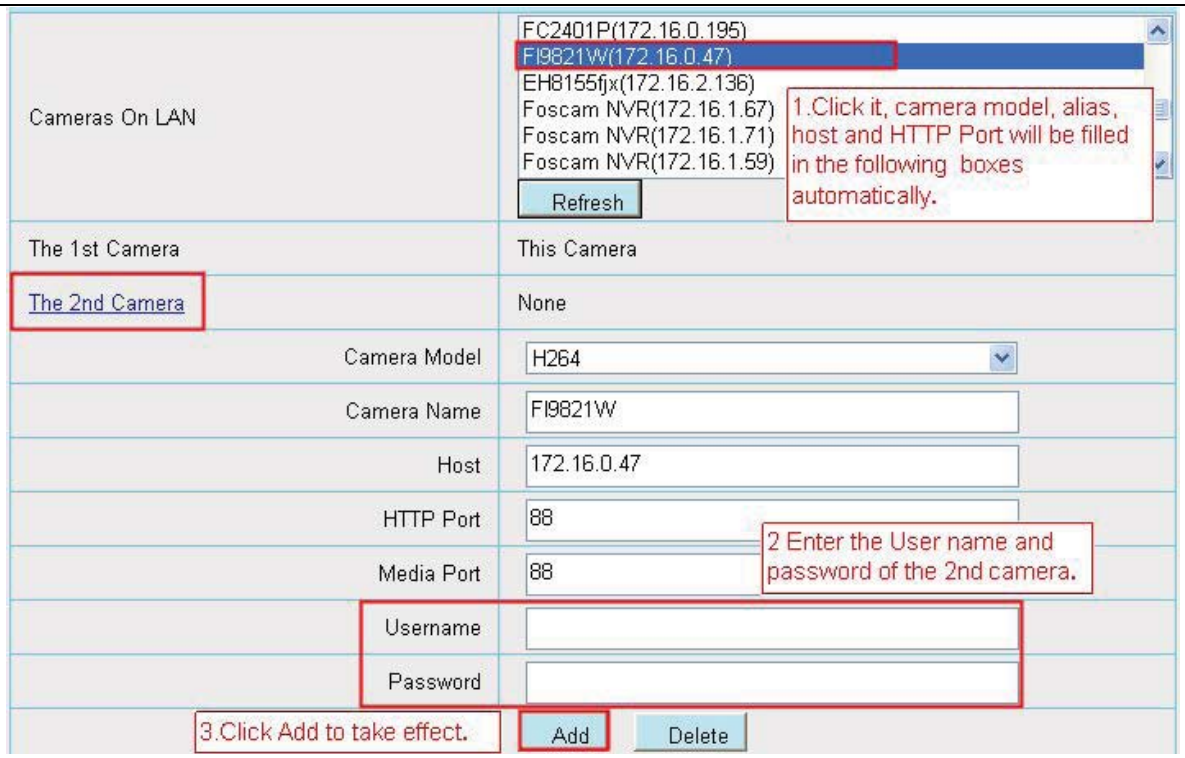


Figure 4.12

Camera Model: Our Company produces two series cameras: MJPEG and H.264. Here will show you which series the camera belongs to.

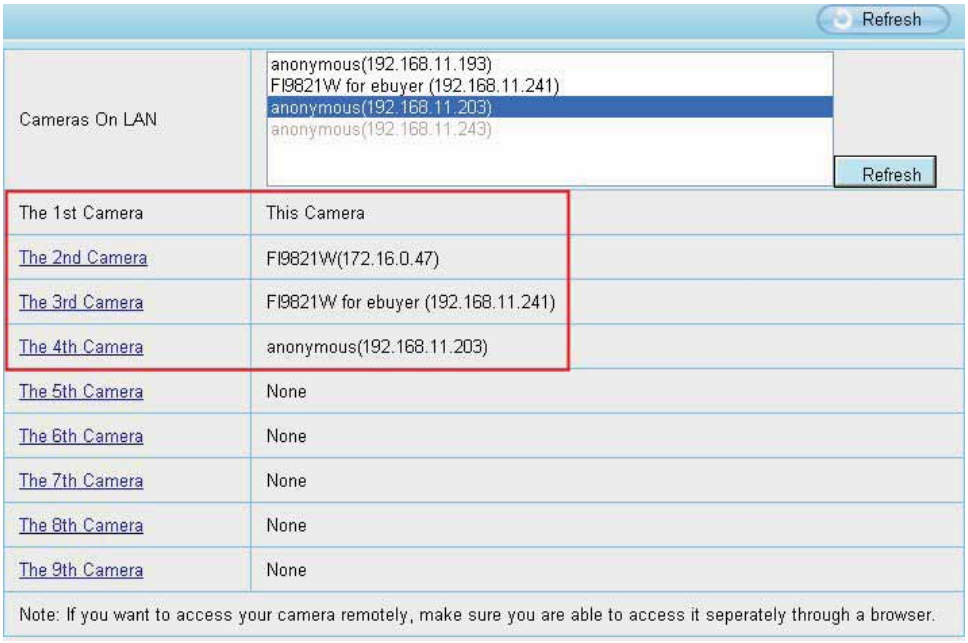


Figure 4.13

Back to Surveillance Windows, and click Four Windows option, you will see four cameras you added.

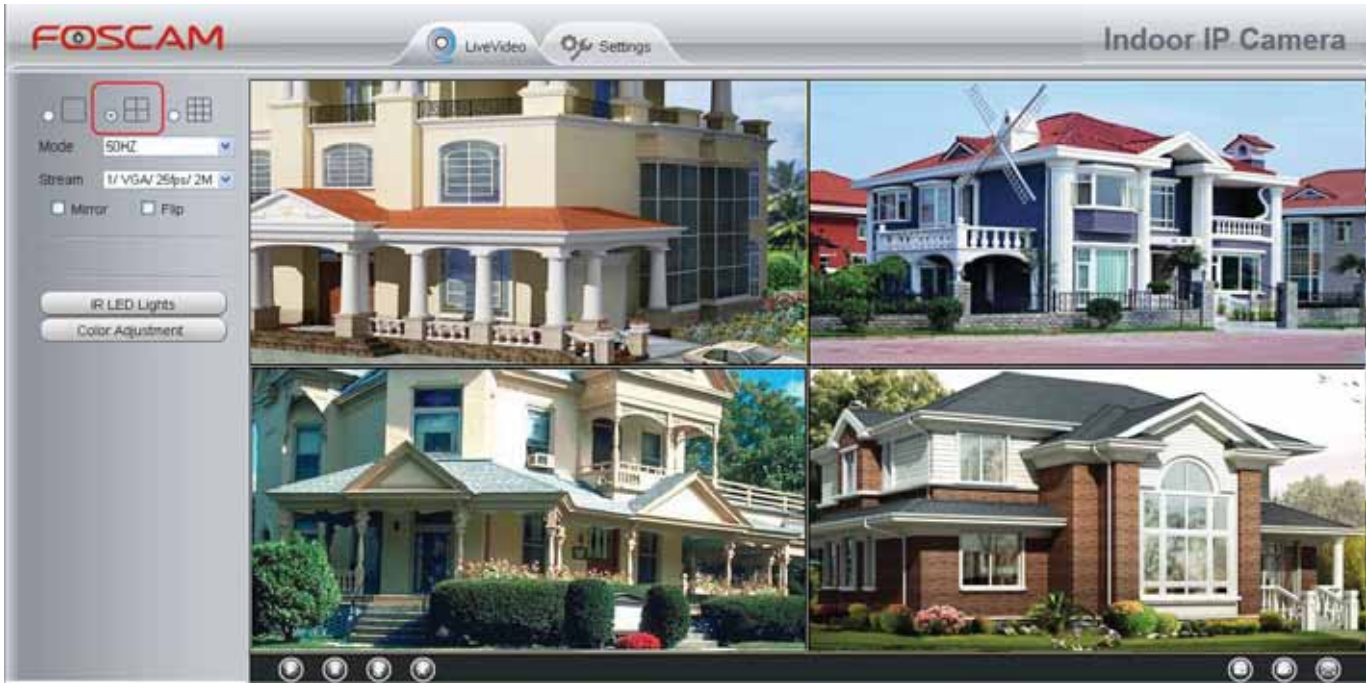


Figure 4.14

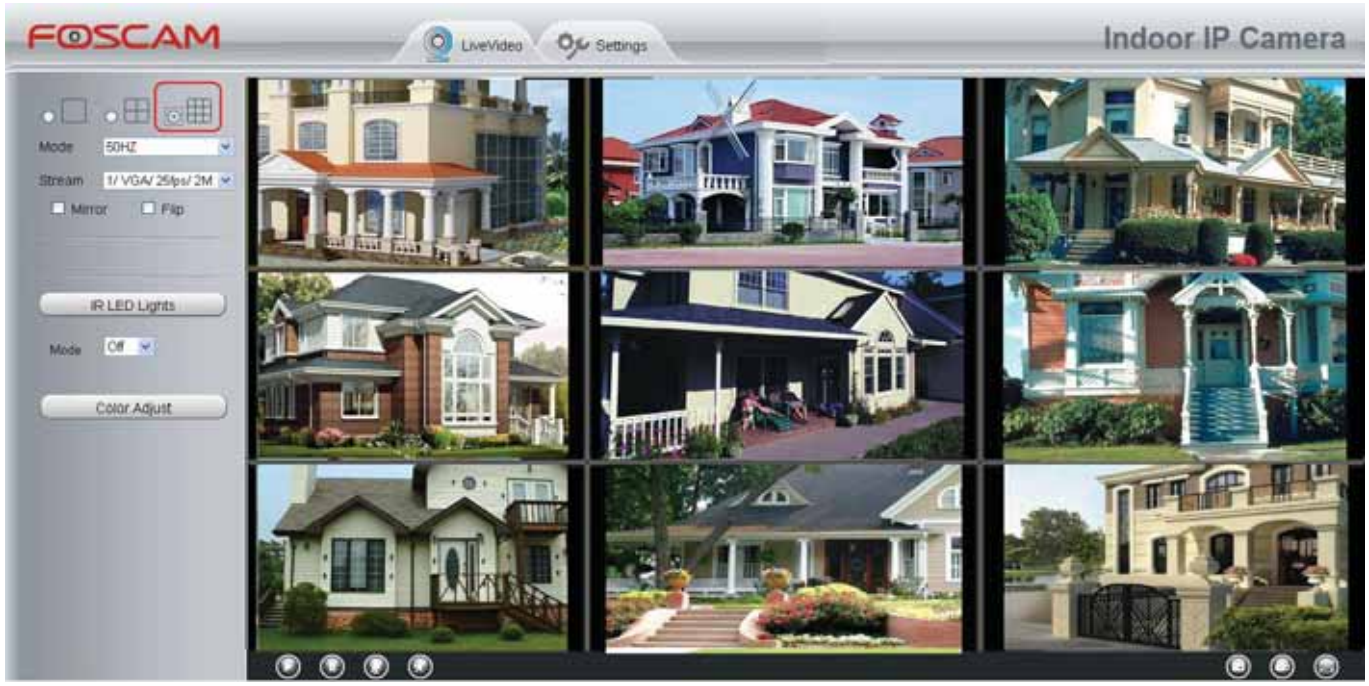


Figure 4.15

Add cameras in WAN

If you want to view all cameras via the internet(remote computer), you will need to add them using DDNS domain name. Firstly, make sure all of the cameras you added can be accessed through the internet. (Read How to configure DDNS settings in chapter 4.3.3)

Login to the first camera using a DDNS domain name and port.

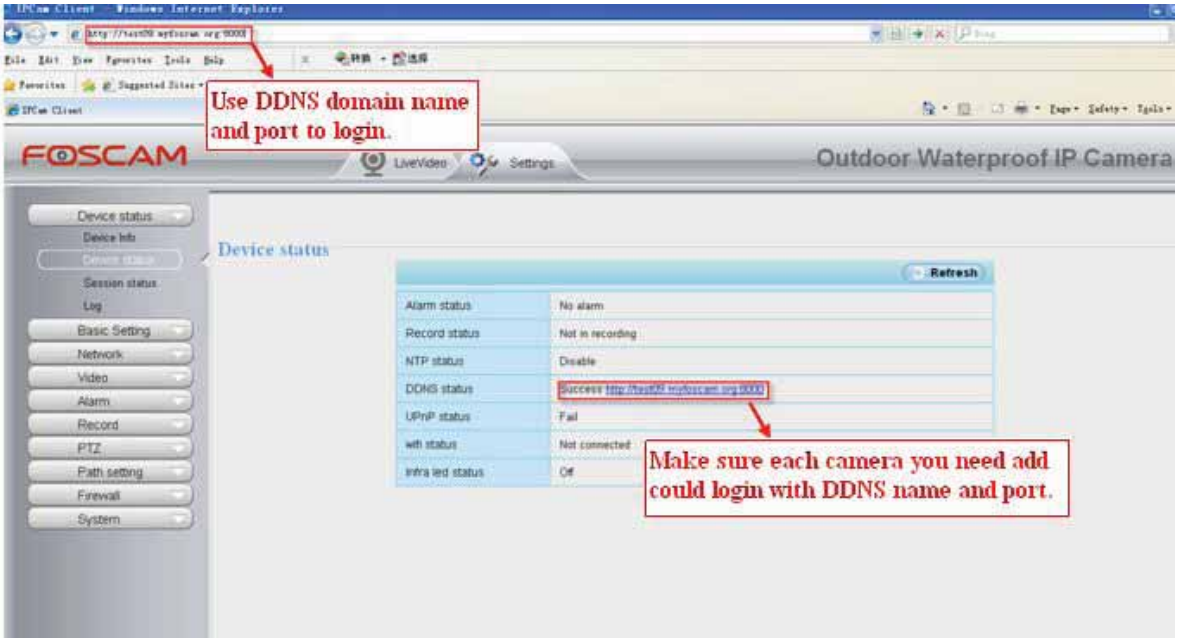


Figure 4.16

Click Multi-Device Settings. Choose The 2nd Device. Fill in the 2nd camera's name, DDNS domain name, port number. Enter user name and password and then choose Add.

Figure 4.17

1----- The camera model: MJ or H264.
2----- The 2nd camera's name
3----- Fill in the 2nd camera's DDNS host not LAN IP
NOTE: The MJ series have the same HTTP Port NO. and Media Port NO.
4 ---- Enter the 2nd camera's user name and password
5---- Click Add button and to take effect
NOTE: Here the Host must be entered as the second camera's DDNS domain name, not its LAN IP.

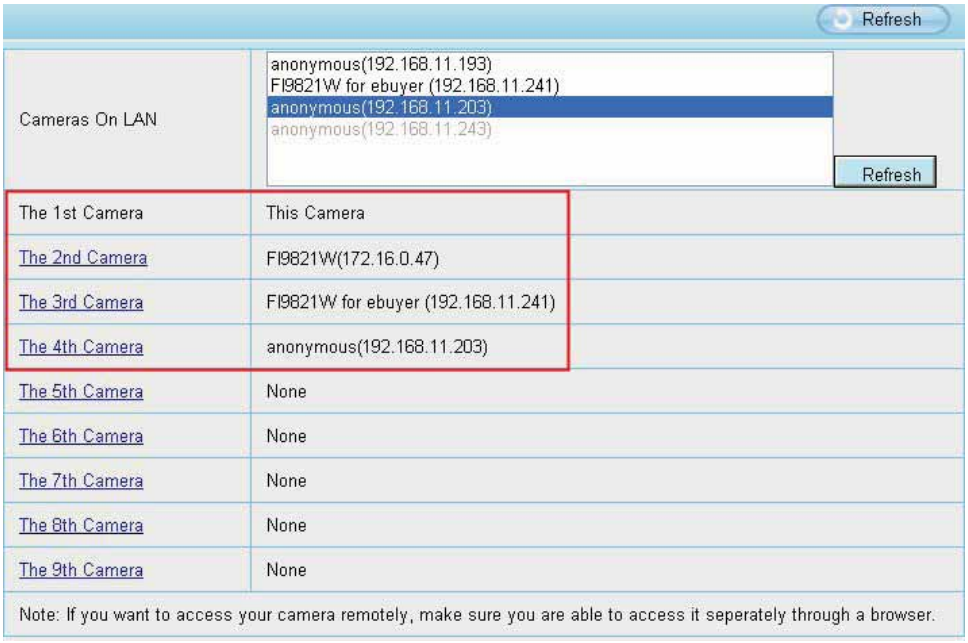


Figure 4.18

Return to video window. You will see all of the cameras accessible through the internet.
When you are away from home, you can use the first camera's DDNS domain name and port to view all the cameras via internet.

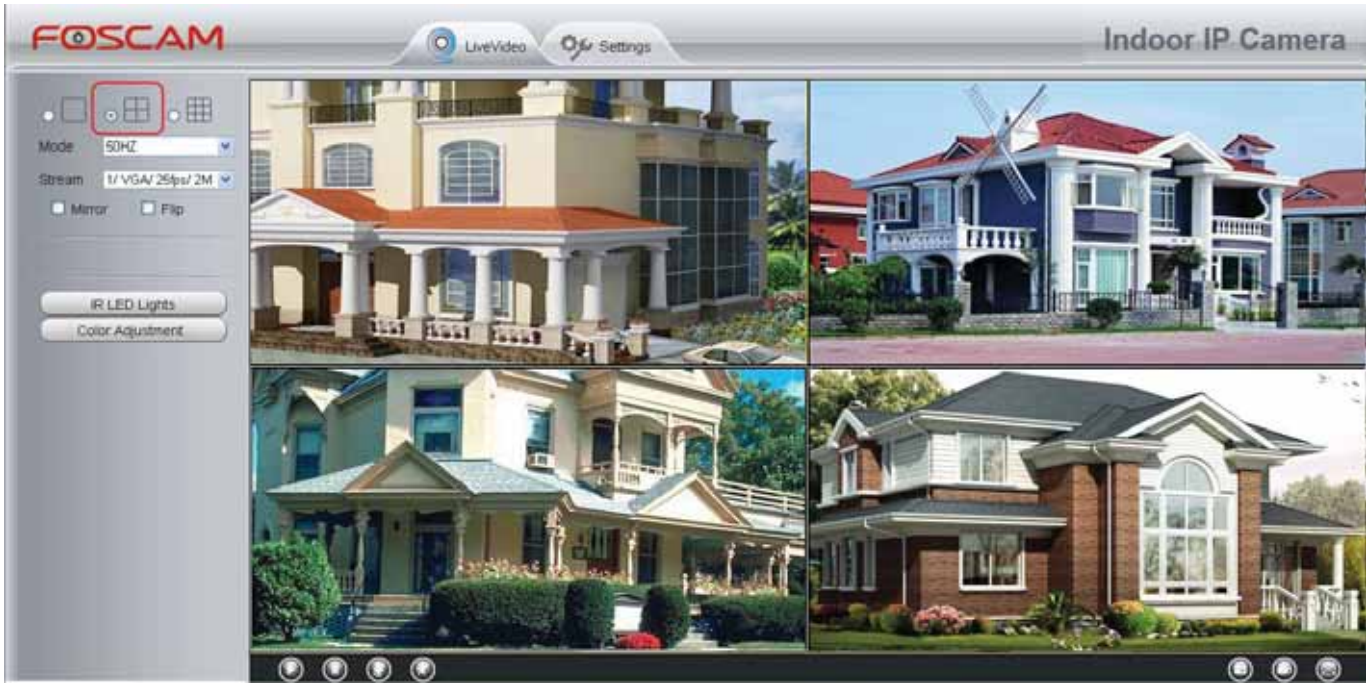


Figure 4.19

4.3 Network

This section will allow you to configure your camera's IP, PPOE, DDNS, UPnP, Port, Mail Settings and FTP Settings.

4.3.1 IP Configuration

If you want to set a static IP for the camera, please go to **IP Configuration** page. Keep the camera in the same subnet of your router or computer.

Figure 4.20

Changing settings here is the same as using the IP Camera Tool. (Figure 4.23/4.24)

It is recommended that you use the subnet mask, gateway and DNS server from your locally attached PC. If you don't know the subnet mask, gateway and DNS server, you can check your computer's local area connection as follows:

Control Panel--Network Connections--Local Area Connections --Choose Support--Details.

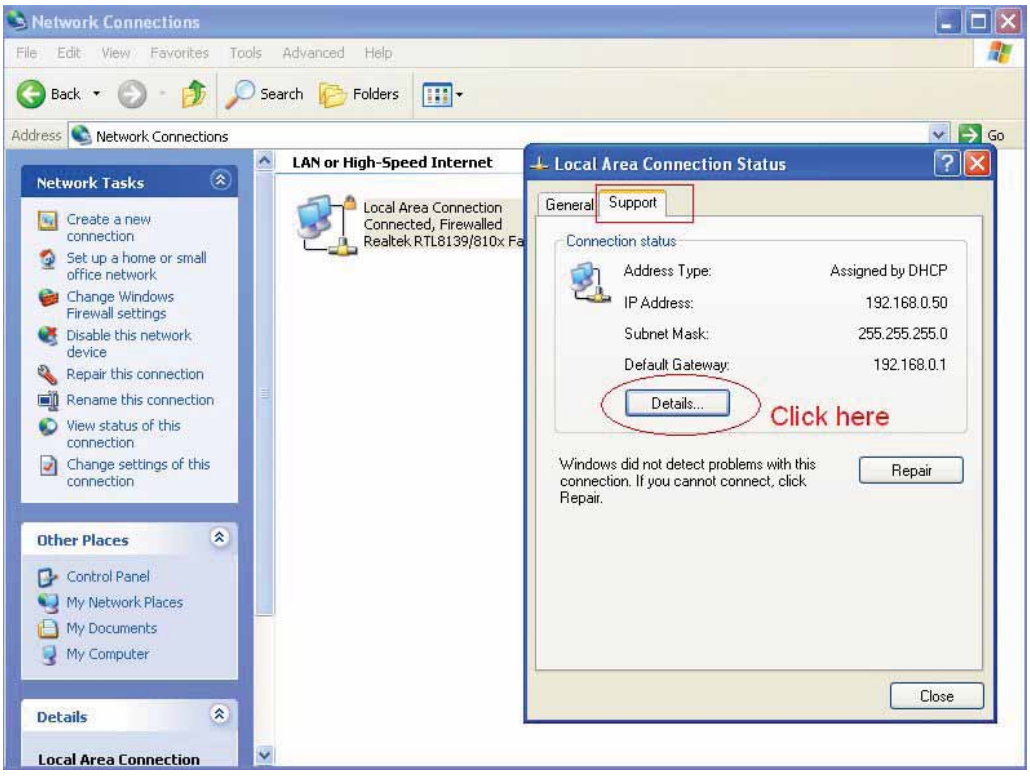


Figure 4.21

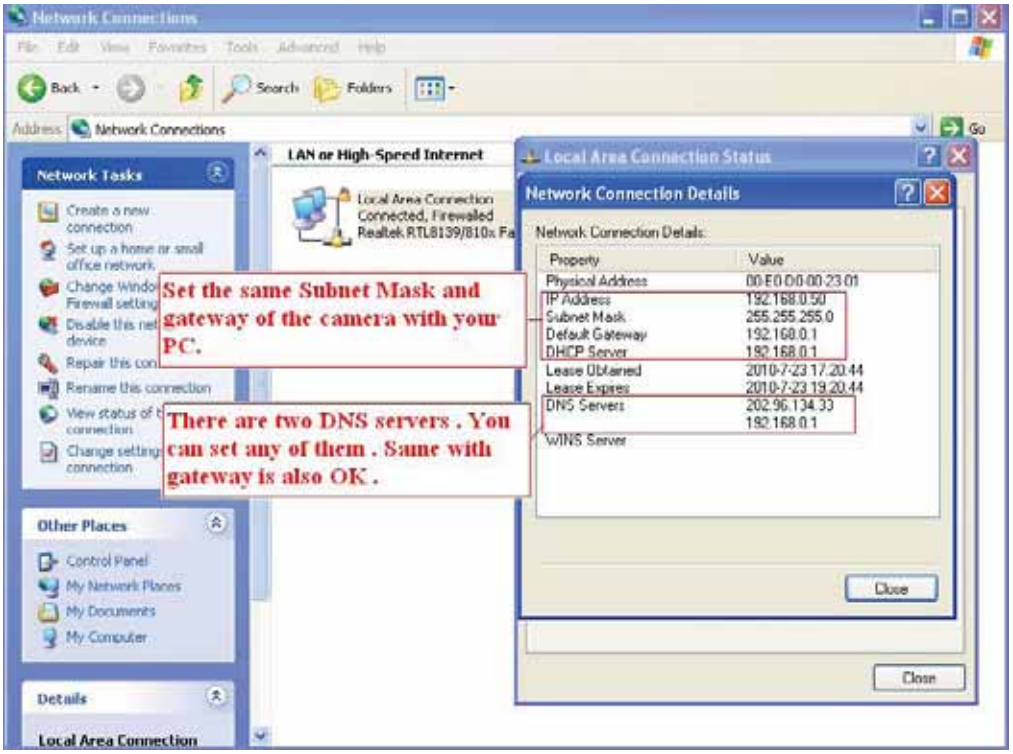


Figure 4.22

If you don't know the DNS server, you can use the same settings as the Default Gateway.

4.3.2 Wireless Settings

Step 1: Choose "Settings" on the top of the camera interface, and go to the "Network" panel on the left side of the screen, then click "Wireless Settings."

Click the Scan button and the camera will detect all wireless networks around the area. It should also display your router in the list (Figure 4.30).

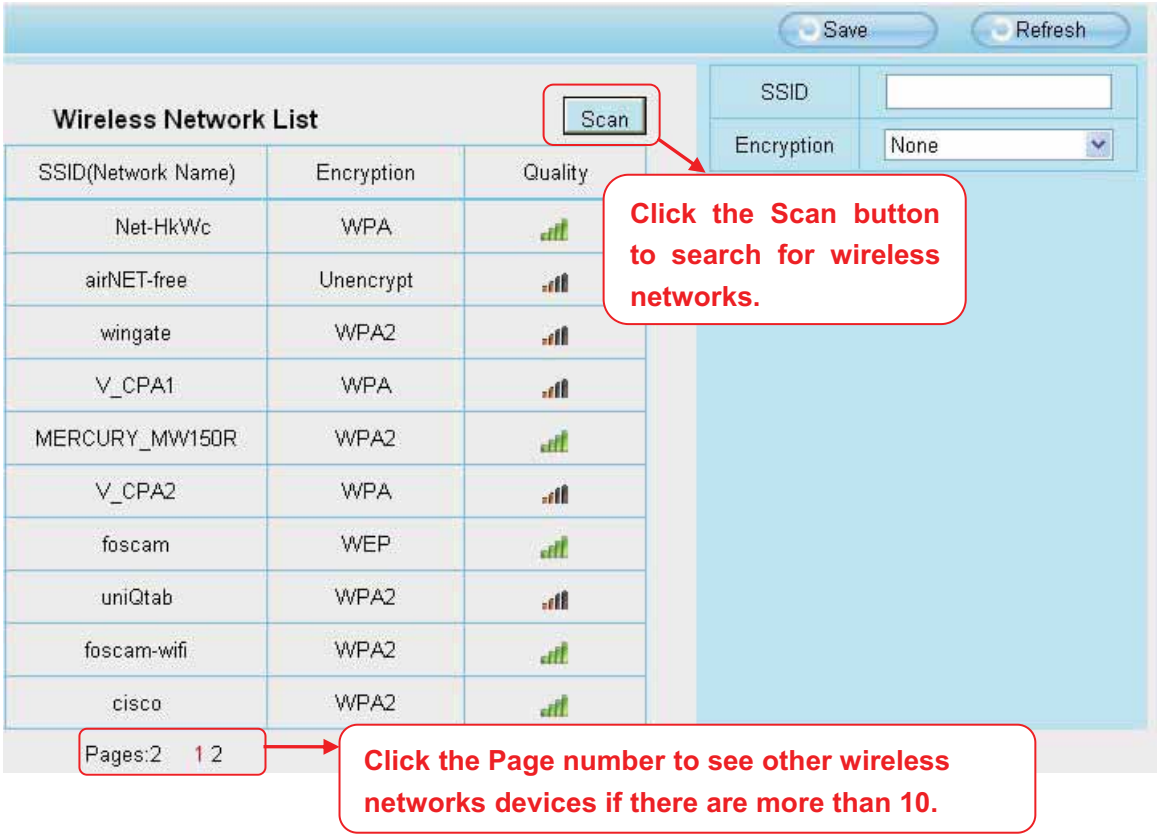


Figure 4.23

Step 2: Click the SSID (name of your router) in the list, the corresponding information related to your network, such as the name and the encryption, will be filled into the relevant fields automatically.

You will only need to fill in the password of your network. Make sure that the SSID, Encryption and the password you filled in are exactly the same for your router.

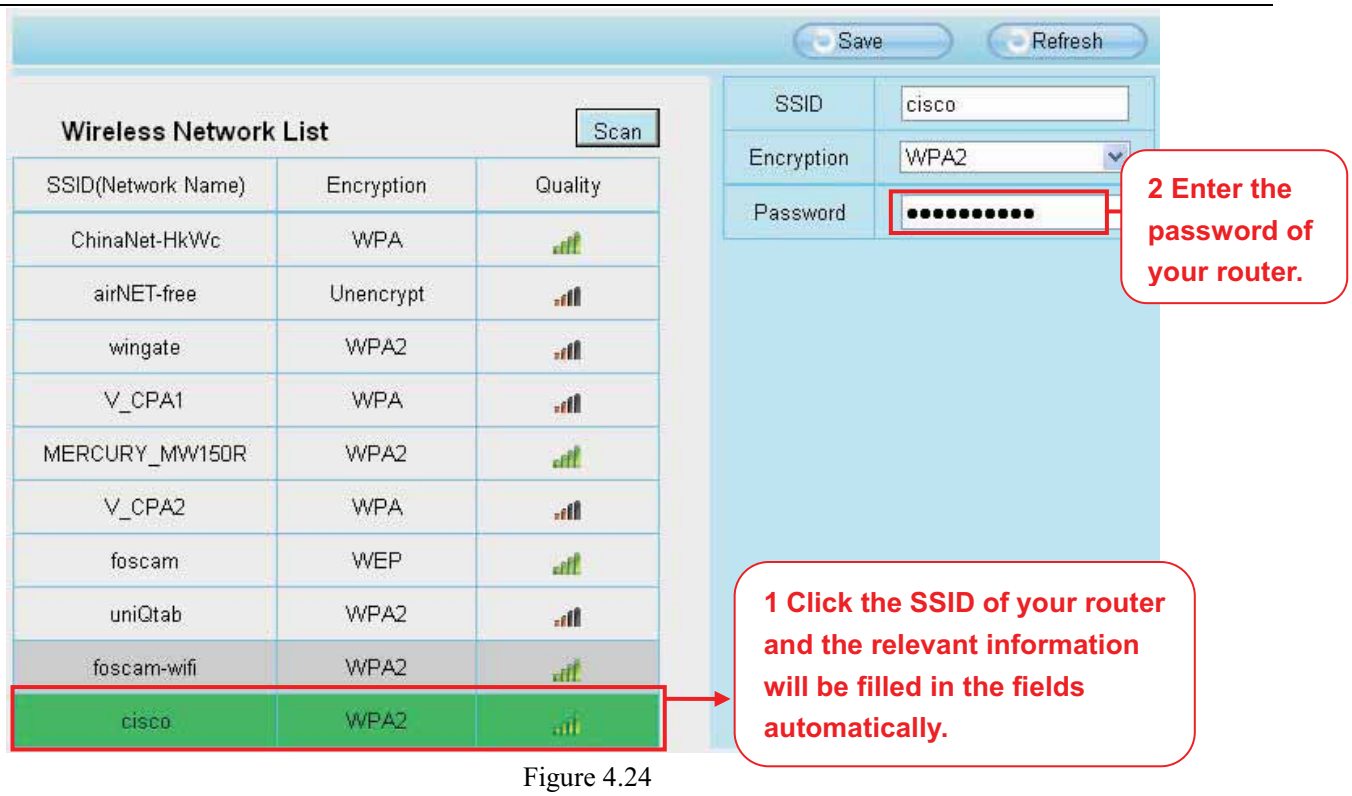


Figure 4.24

Step 3: Please click on the Save button after all settings have been entered and disconnect the network cable. Never shut down the power of the camera until the IP camera is able to connect to the wireless network.

The LAN IP address will disappear on the window of IP Camera Tool when the camera is configuring a wireless connection. Wait about 1 minute, the camera should obtain a wireless connection, and the LAN IP of the camera will show again on the window of the IP Camera Tool. The IP address may have changed after the camera receives a wireless connection; we recommend setting a static local IP address if this IP address changes by right clicking the camera in IP Camera Tools, setting a static IP, and pushing OK.

Congratulations! You have set up the wireless connection of the camera successfully.

4.3.3 PPPoE

If you are using a PPPoE connection, enable it and enter the User Name and Password for your PPPoE account.

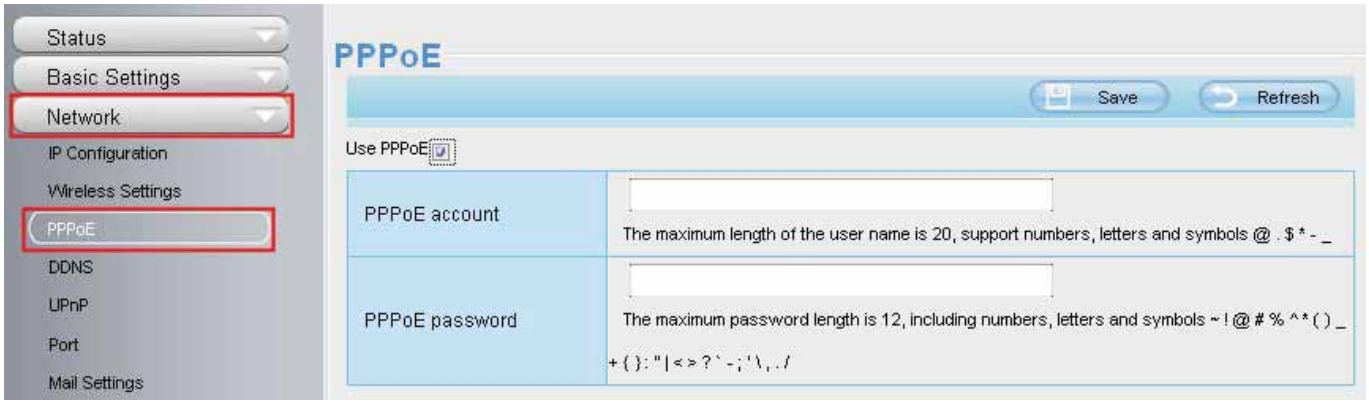


Figure 4.25

4.3.4 DDNS

FOSCAM camera has embedded a unique DDNS domain name when producing, and you can directly use the domain name, you can also use the third party domain name.

FOSCAM domain name

Here take **cp4911.myfoscam.org** for example. Go to option of DDNS on the **Settings->Network** panel, you can see the domain name.

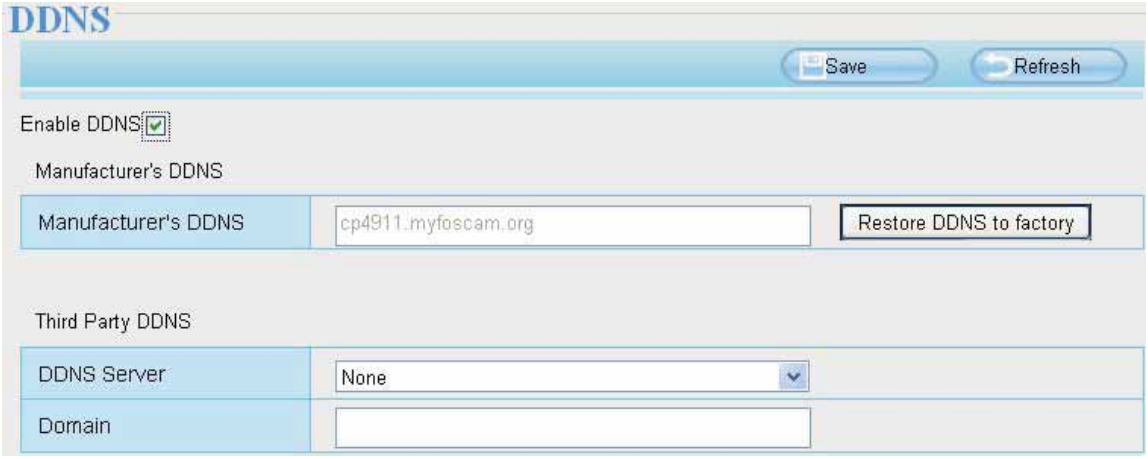


Figure 4.26

Now you can use **http:// Domain name + HTTP Port** to access the camera via internet.

Take hostname **cp4911.myfoscam.org** and HTTP Port no. 8000 for example, the accessing link of the camera via internet would be **http://cp4911.myfoscam.org:8000**

Restore DDNS to factory: If you have configured Third Party DDNS successfully, but you want to use Manufacturer's DDNS again , here click this button and start Manufacturer's DDNS Service.

Third Party Domain Name Settings

User can also use third part DDNS, such as www.no-ip.com. ,www. 3322.com

Here take **www.no-ip.com** for example :

① Step 1 Go to the website www.no-ip.com to create a free hostname

Firstly: Login on **www.no-ip.com** and click No-IP Free to register.

Figure 4.27

Please register an account step by step according to instructions on **www.no-ip.com**

After registration, please login your email which used to register. You will receive an email from website, please click the link to activate your ACCOUNT as indicated in email.

Secondly: Login the link with the registered username and password to create your domain name.

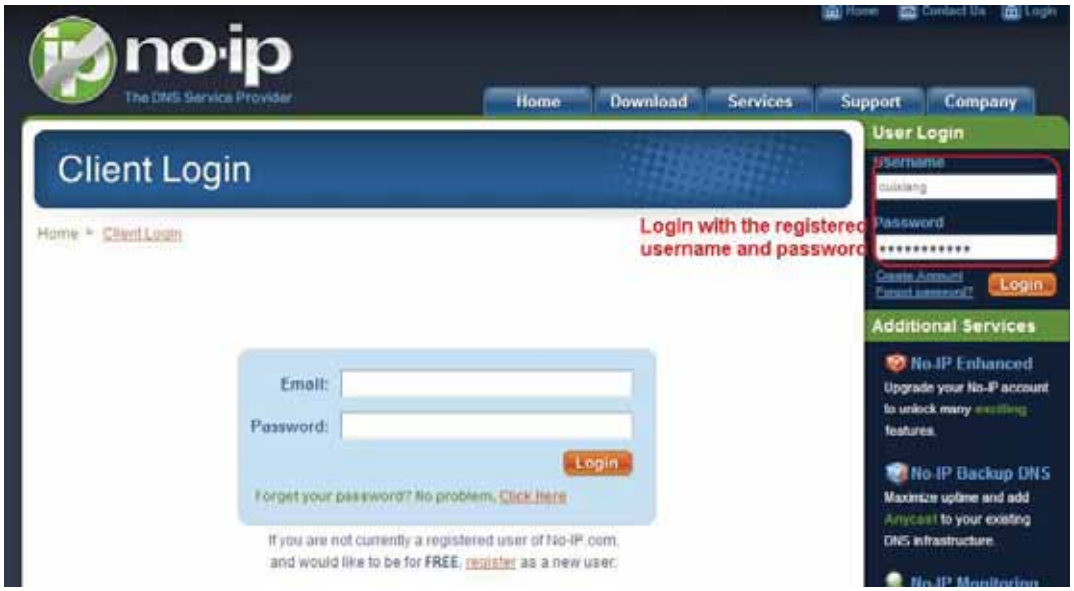


Figure 4.28

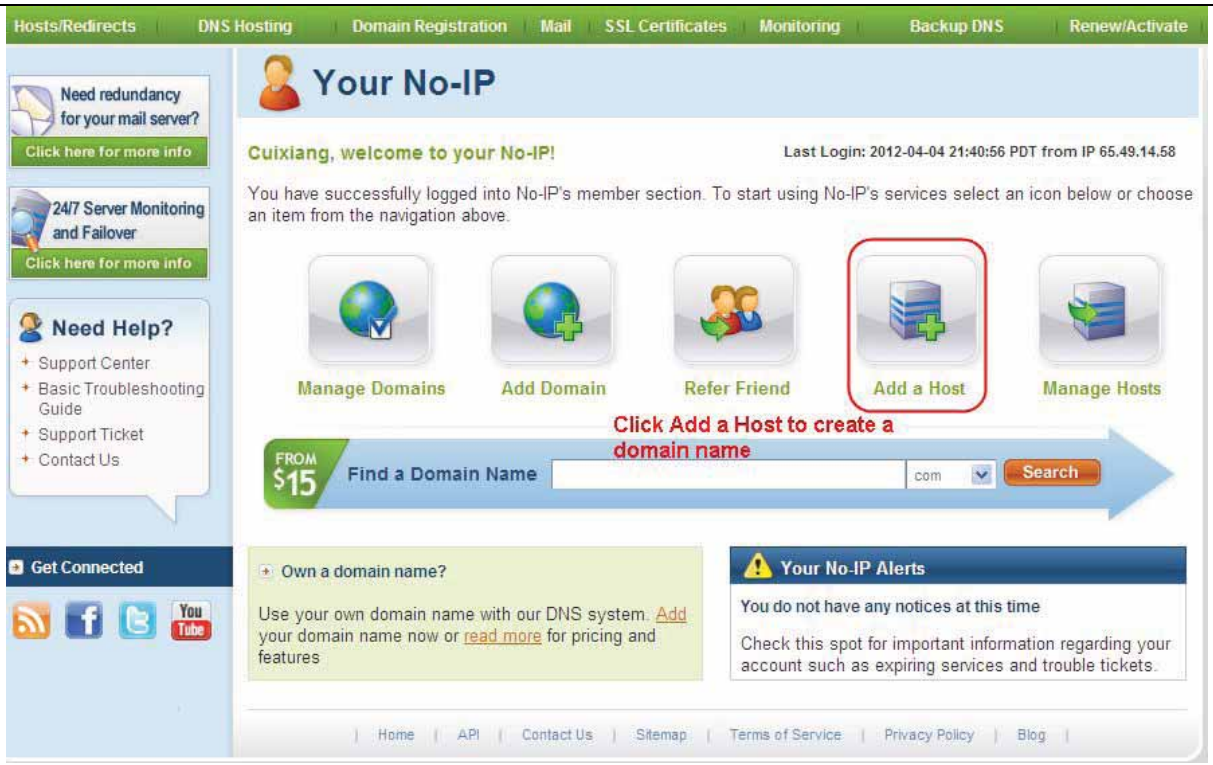


Figure 4.29

Please create the domain name step by step according to instructions on www.no-ip.com

Step 2 DO DDNS Service Settings within the Camera

Please set DDNS Settings within the camera by hostname, a user name and password you've got from **www.no-ip.com**

Take hostname ycxgwp.no-ip.info, user name **foscam**, password **foscam2012** for example.

Firstly, goes to option of DDNS Settings on the administrator panel.

Secondly, select No-Ip as a server.

Thirdly, fill foscam as DDNS user, fill password foscam2012 as DDNS password, fill ycxgwp.no-ip.info as DDNS domain and server URL, Then click save to make effect. The camera will restart and to take the DDNS settings effective.

Fourthly, after the restart, login the camera, and go to option of Device Status on the administrator panel, and check if the DDNS status is successful.

If failed, please double check if you have input the correct hostname, user name, and password, and try to redo the settings.

NOTE :

If you have set Third Party DDNS successfully ,the Foscam Domain Name will be invalid. The Third Party DDNS and the Foscam Domain Name cannot work at the same time, the last time you configured will take effect.

② Do port forwarding within the router

Example: The camera's LAN IP address is http://192.168.8.100:2000

Firstly, login the router, goes to the menu of Port Forwarding or Port Trigger (or named Virtue Server on some brands of router). Take Linksys brand router as an example, Login the router, and goes to Applications & Gaming->Single Port Forwarding.

Secondly, Create a new column by LAN IP address & HTTP Port No. of the camera within the router showed as below.

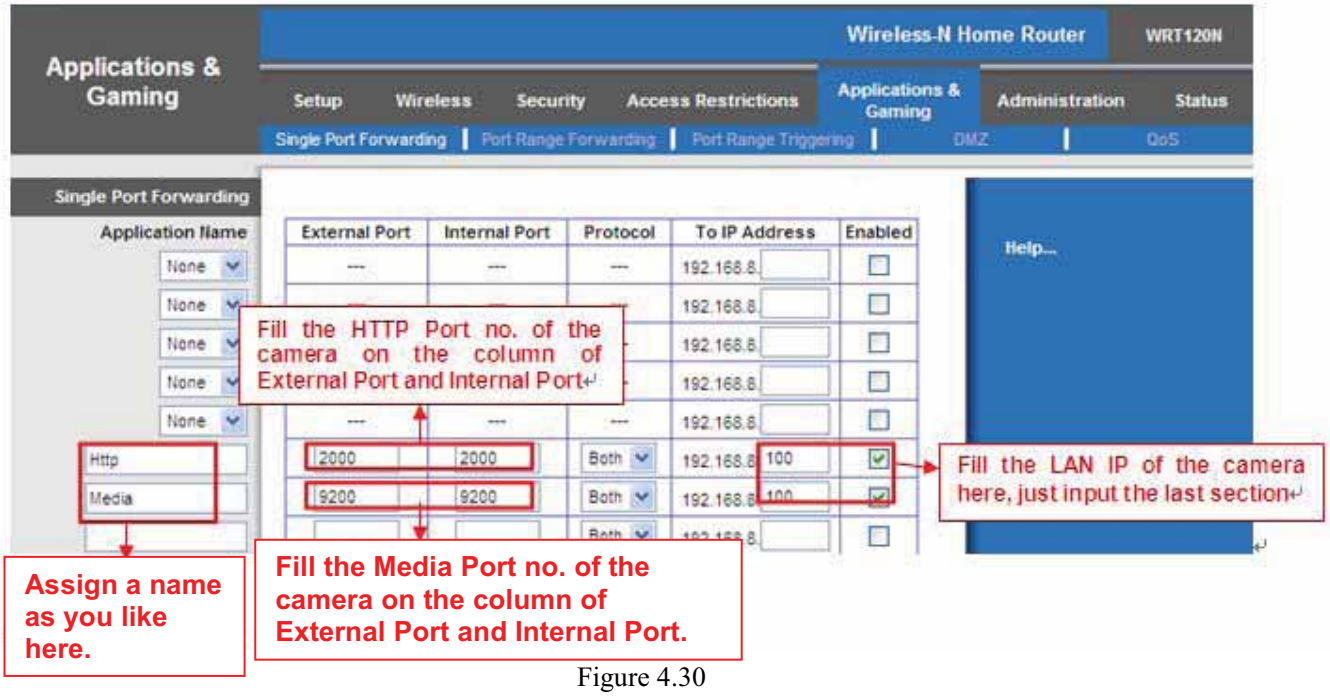


Figure 4.30

③ Use domain name to access the camera via internet

After the port forwarding is finished, you can use the **domain name+ http no.** to access the camera via internet. Take hostname ycxgwp.no-ip.info and http no. 2000for example, the accessing link of the camera via internet would be http:// ycxgwp.no-ip.info:2000

4.3.5 UPnP

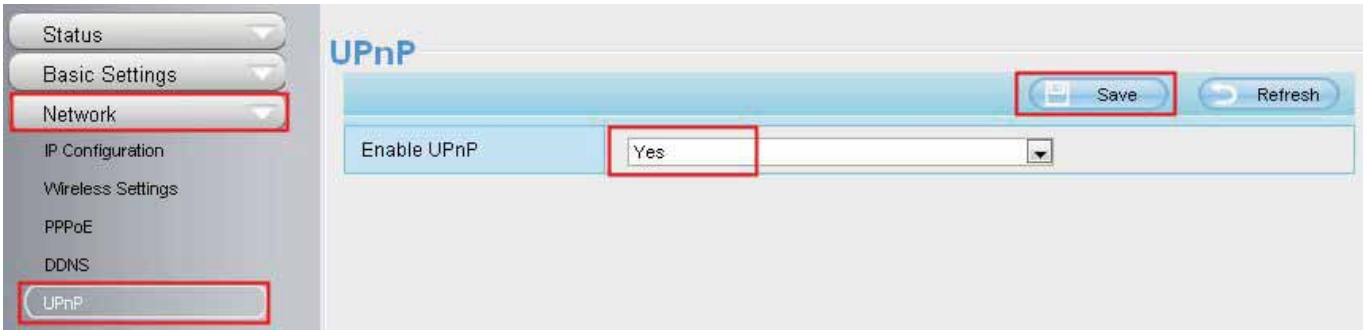


Figure 4.31

The default UPnP status is closed. You can enable UPnP, then the camera's software will be configured for port forwarding. Back to the "Device Status" panel, you can see the UPnP status:

Figure 4.32

The camera's software will be configured for port forwarding. There may be issues with your routers security settings, and sometimes may error. We recommend you configure port forwarding manually on your router (Figure 4.30).

4.3.6 Port

This camera supports HTTP Port / HTTPS Port/ ONVIF Port. HTTP Port is used to access the camera remotely.

HTTP port : By default, the HTTP is set to 88. Also, they can be assigned with another port number between 1 and 65535. But make sure they can not be conflict with other existing ports like 25, 21.

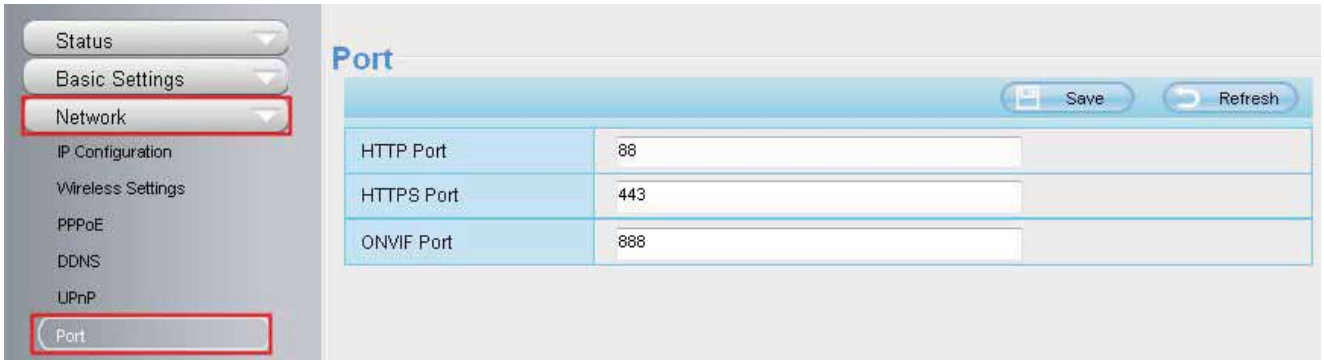


Figure 4.33

Another way to change the HTTP port NO.

Step 1: Open the IP Camera Tool, select the camera you would like to change the port of, right click on the IP address, and click on "Network Configuration", this brings up the network configuration box as shown in Figure 4.32 and 4.33.

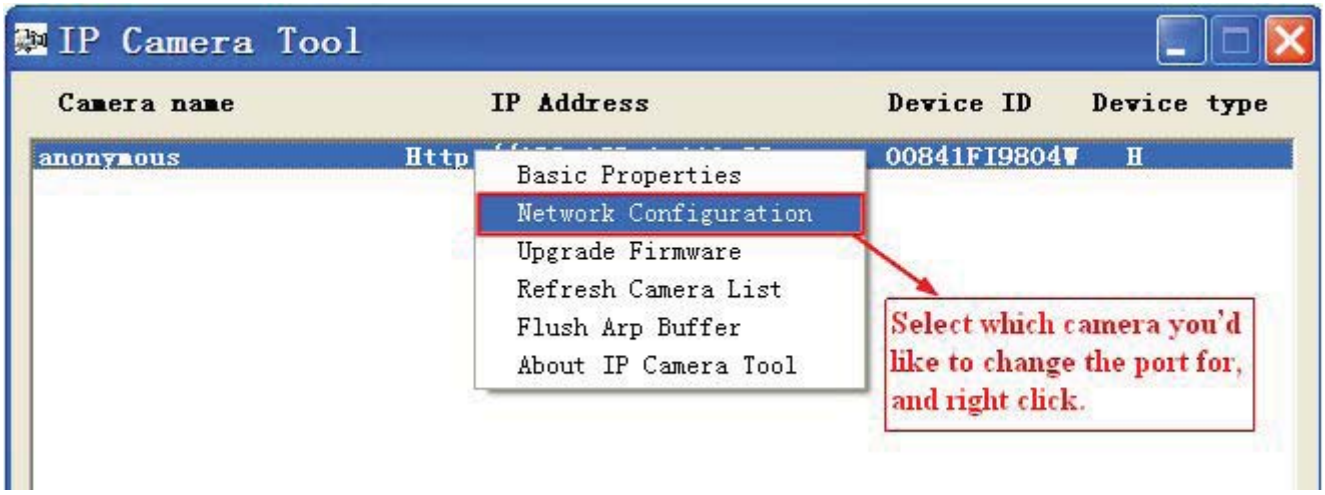


Figure 4.34

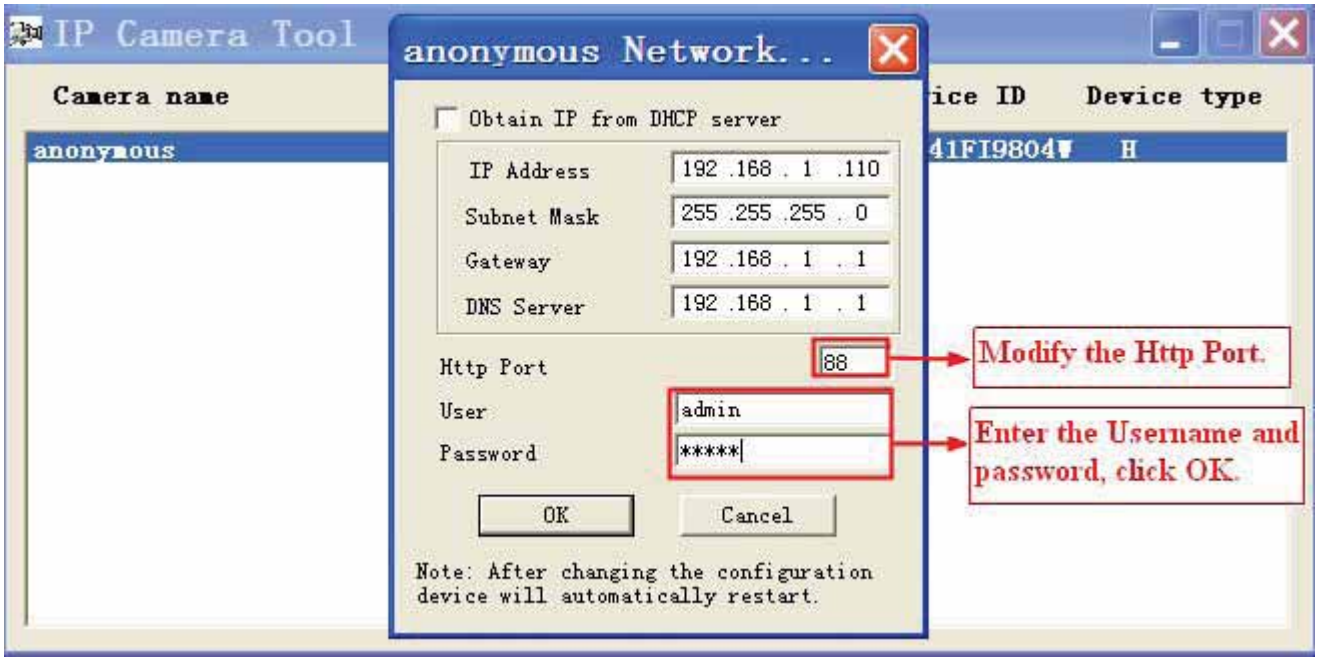


Figure 4.35

Step 2: Enter the username and password of the Administrator (default username is admin with a blank password), and click “OK” to apply changes.

Step 3: Wait around 10 seconds, you’ll see that the camera’s LAN IP address has changed. In our example it was changed to 2000, so we see http://192.168.8.102:2000 in IP Camera Tool. Also, the LAN IP address is now fixed at a static IP address of http://192.168.8.102:2000. This IP address will not change even if the camera is powered off and back on, the camera will remain on this LAN IP address. This is very important that a static LAN IP address is set, or you may have problems later with remote access and seeing the camera remotely if the camera loses power and reconnects on a different LAN IP address. Make sure you set a static LAN IP address!

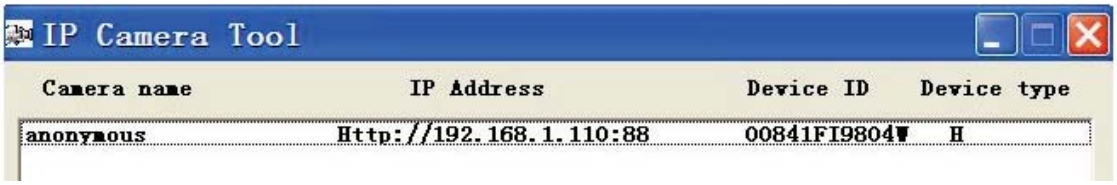


Figure 4.36

NOTE: If the camera cannot be accessed, please make sure the port forwarding is succeed.

HTTPS port: The default port is 443. You can use the url to access the camera: https:// IP + HTTPS port.
Sometimes you need to add the url to the Trusted Sites,
Open Internet Explorer if it is not already opened. Click on Tools, then click Internet Options.
Next, click the Security tab, then click the Trusted sites button.

Figure 4.37

ONVIF port: By default, the ONVIF port is set to 888. Also, they can be assigned with another port number between 1 and 65535(except 0 and 65534). But make sure they can not be conflict with other existing ports.

RTSP function

RTSP URL rtsp:// [user name][:password]@IP:HTTP port number/videosream

The part in the square brackets may be omitted.

user name & password: The user name and password to access the camera. This part can be omitted.

IP: WAN or LAN IP address.

Videostream: Here support three mode: videoMain, videoSub and audio. When the network speed is bad,

here you had better select videoSub. If you select audio, you can only hear the sound but cannot see the video.

For example:
IP: 192.168.1.11
HTTP Port number: 88
User name: admin
Password: 123

Here I can enter one of the following URLs in the VLC.
1. rtsp://admin:123@192.168.1.11:88/videoMain
2. rtsp:// @192.168.1.11:88/videoMain
3. rtsp://:123@192.168.1.11:88/videoMain
4. rtsp://admin@192.168.1.11:88/videoMain

Open the VLC, and go to Media(Open Network Stream option, then enter the URL into VLC.

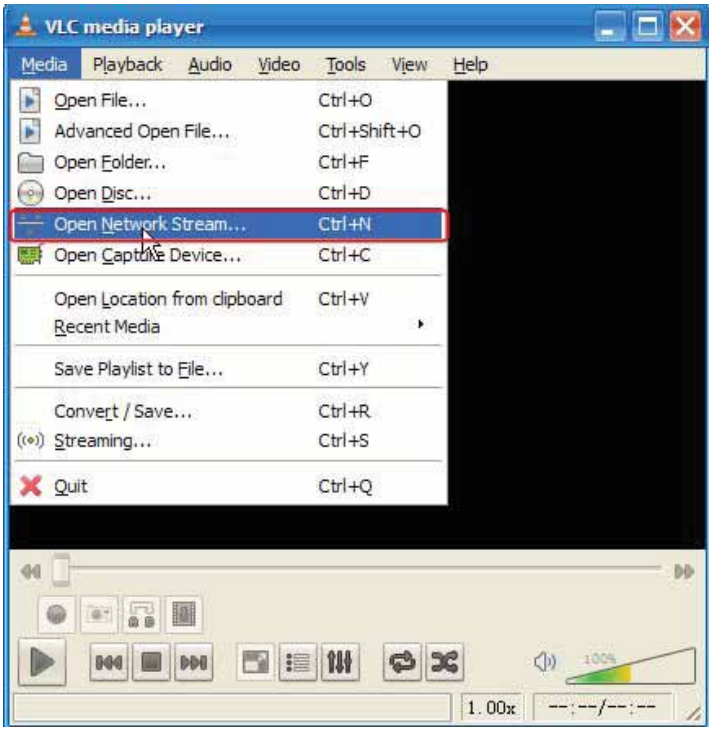


Figure 4.38

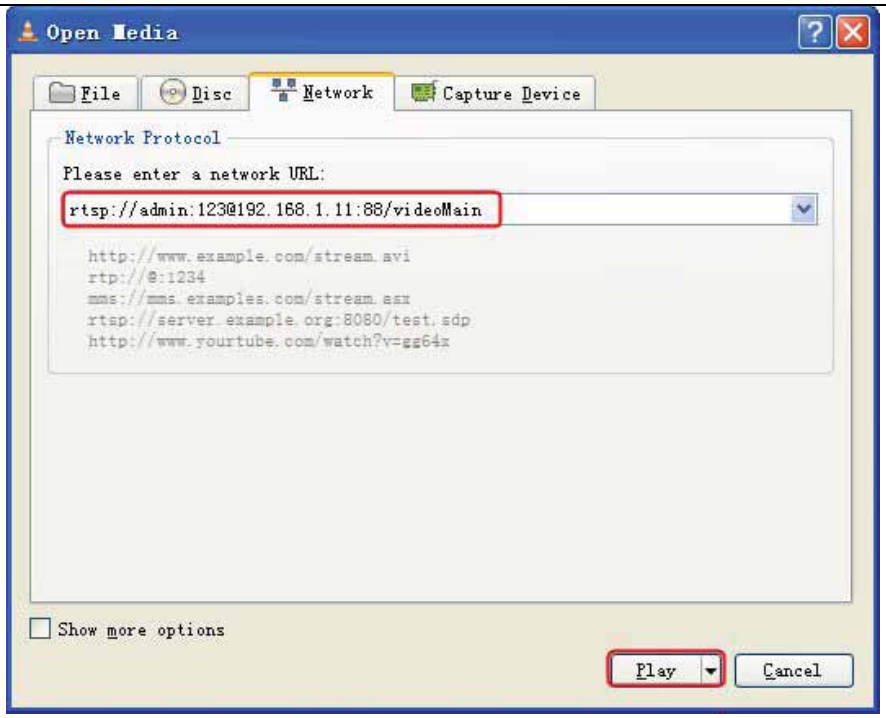


Figure 4.39

Sometimes you may need to enter the user name and password again. Click OK and you can see the real-time preview.

Figure 4.40

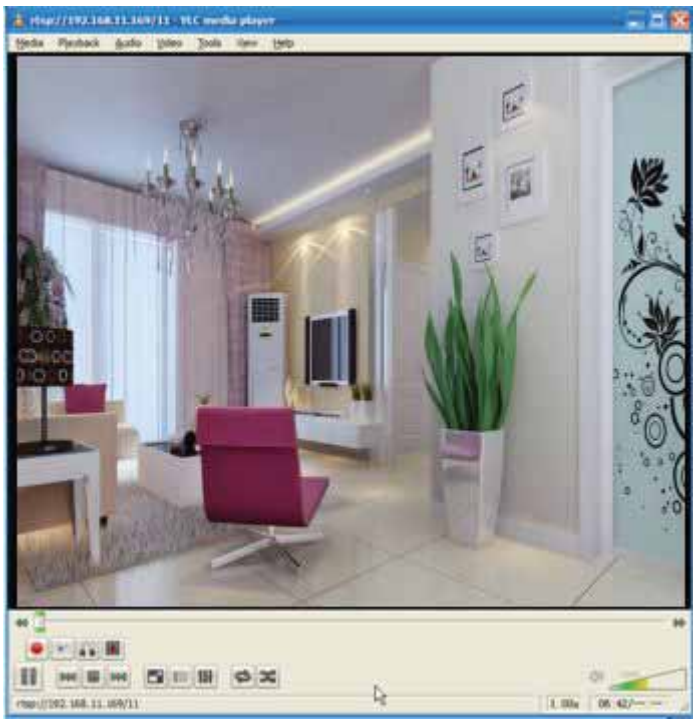


Figure 4.41

If you cannot play the video in the VLC player, please check the port mapping. You can read Quick Installation Guide about How to configure port forwarding.

NOTE:
If you modify the camera's username or password, you had better reboot the camera, or else the new username and password cannot take effect when you enter the authentication in the VLC.

4.3.7 Mail Settings

If you want the camera to send emails when motion has been detected, here Mail will need to be configured.

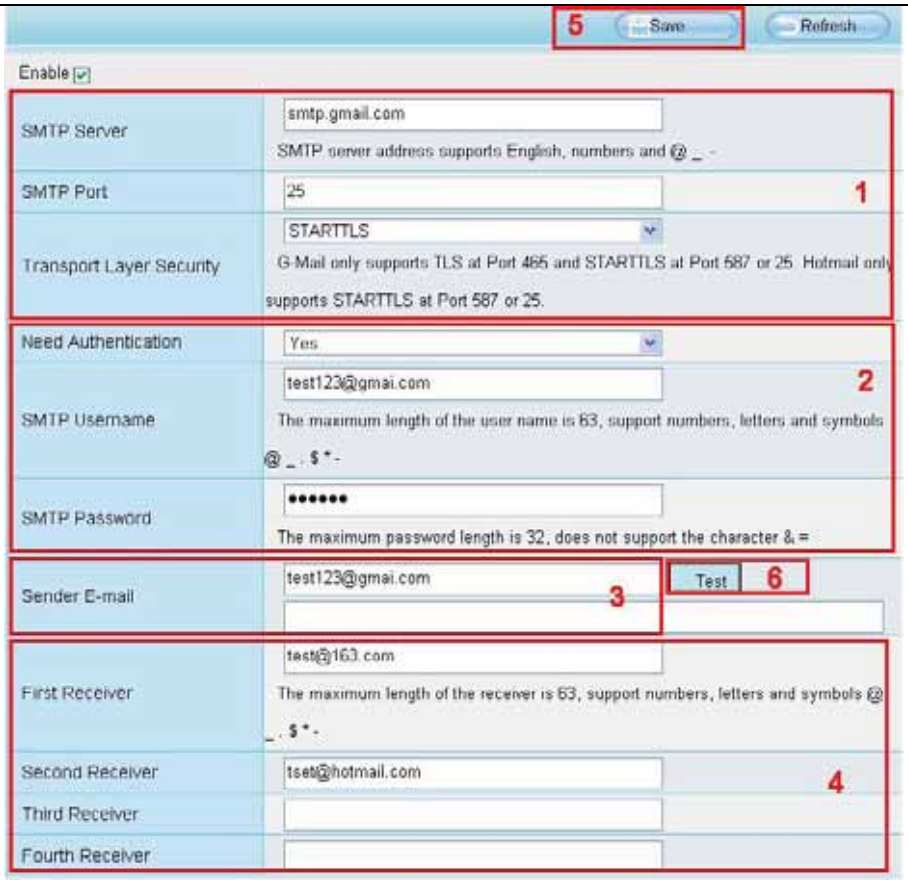


Figure 4.42

1----- SMTP Server/ Port /Transport Layer Security Enter SMTP server for sender. SMTP port is usually set as 25. Some SMTP servers have their own port, such as 587 or 465, and Transport Layer Security usually is None. If you use Gmail, Transport Layer Security must be set to TLS or STARTTLS and SMTP Port must be set to 465 or 25 or 587, which port you choose should be decided by which Transport Layer Security you select.

2-----SMTP Username/ password: ID account and password of the sender email address

3----- Sender E-mail Mailbox for sender must support SMTP

4----- Receiver Mailbox for receiver need not support SMTP, you can set 4 receivers

5----- Save Click Save to take effect

6----- Test Click Test to see if Mail has been successfully configured.

Click Test to see if Mail has been successfully configured.

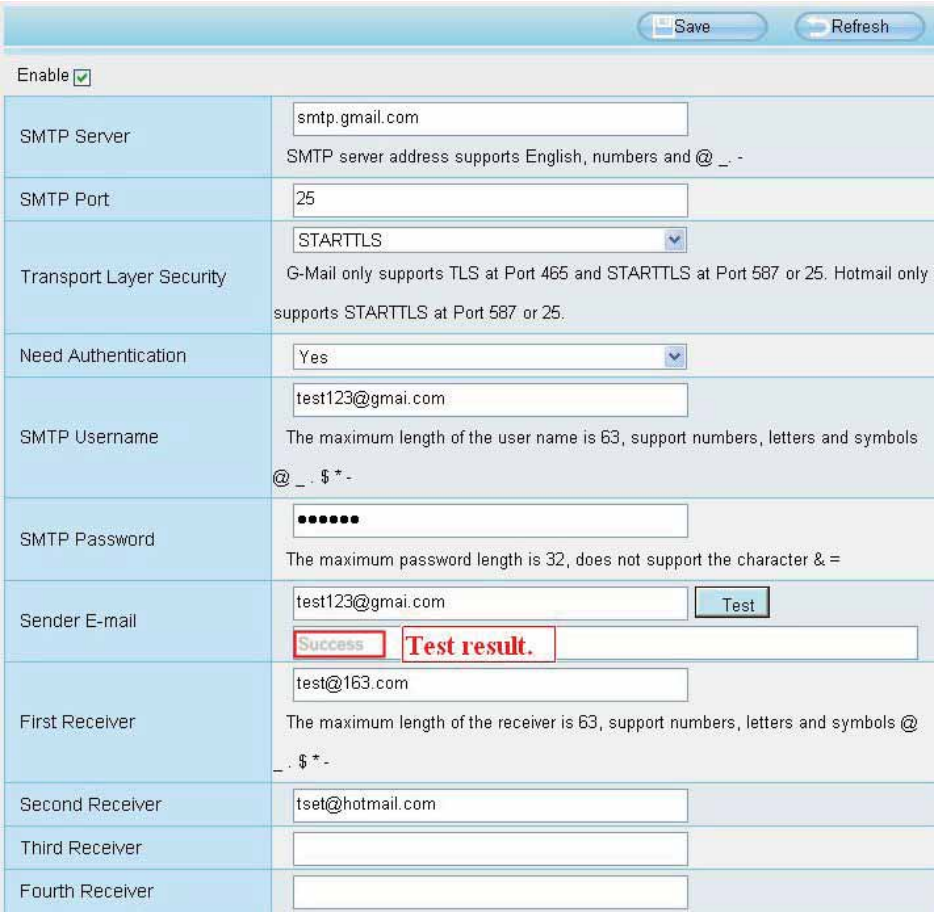


Figure 4.43

If the test success, you can see the Success behind the Test, at the same time the receivers will receive a test mail.

If the test fails with one of the following errors after clicking Test, verify that the information you entered is correct and again select Test .
1) Cannot connect to the server
2) Network Error. Please try later
3) Server Error
4) Incorrect user or password
5) The sender is denied by the server. Maybe the server need to authenticate the user, please check it and try again
6) The receiver is denied by the server. Maybe because of the anti-spam privacy of the server
7) The message is denied by the server. Maybe because of the anti-spam privacy of the server
8) The server does not support the authentication mode used by the device

4.3.8 FTP Settings

If you want to upload record images to your FTP server， you can set **FTP Settings.**

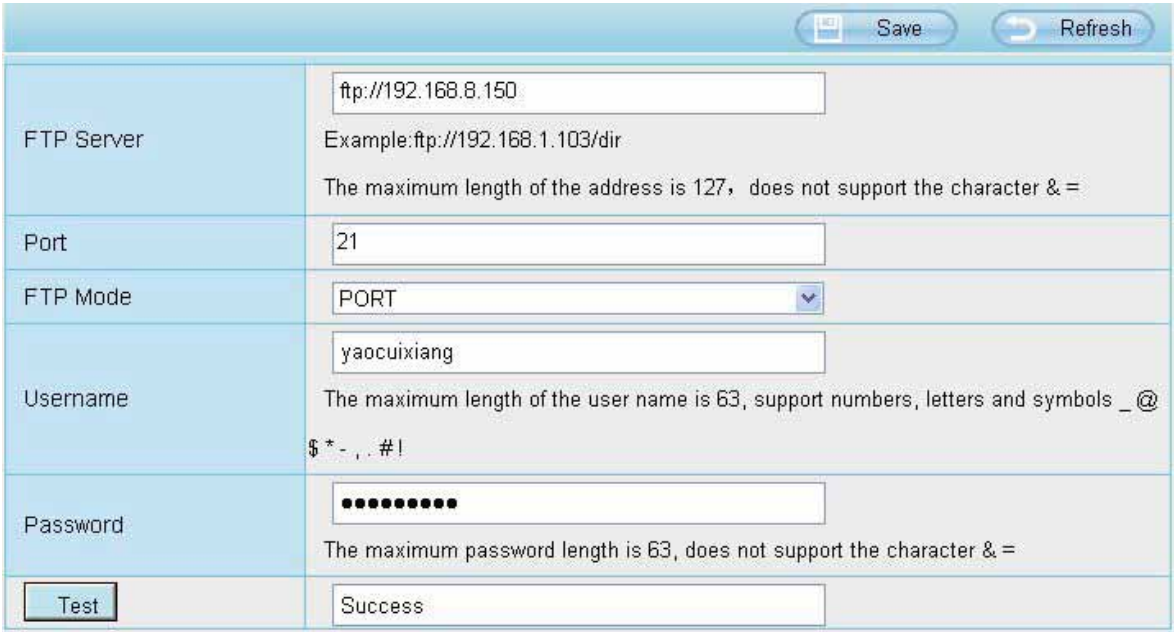


Figure 4.44

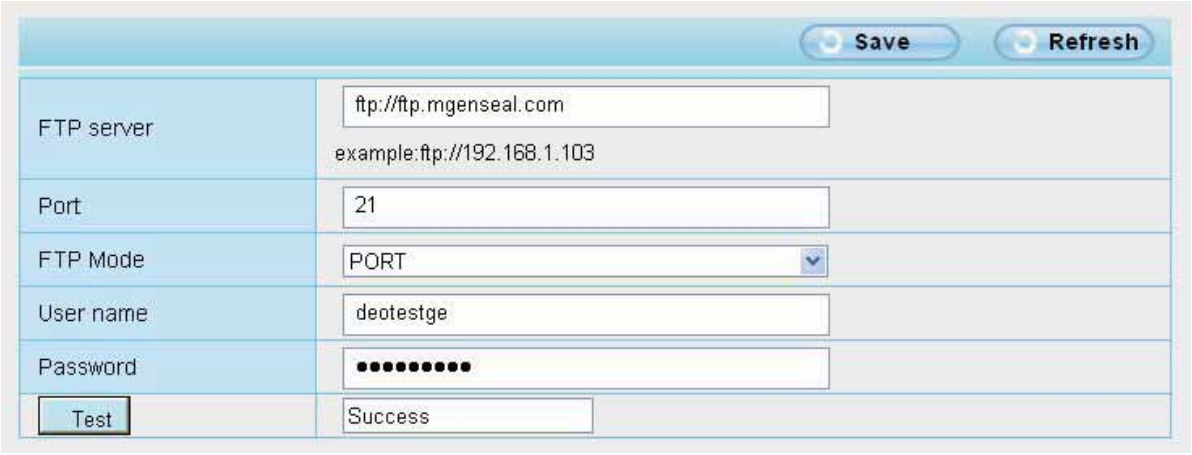


Figure 4.45

FTP server: If your FTP server is located on the LAN, you can set as Figure 4.43.
If you have an FTP server which you can access on the internet, you can set as Figure 4.44.
Port: Default is port 21. If changed, external FTP client program must change the server connection port accordingly.
FTP Mode: Here supports two modes: PORT and PASV.
Username/password: The FTP account and password.
Click Save to take effect.
Click Test to see if FTP has been successfully configured.

4.3.9 P2P

Access the camera by smart phone (Android or iOS operating system)
First of all, you need to open the P2P function of the camera at “Settings-->Network-->P2P.”

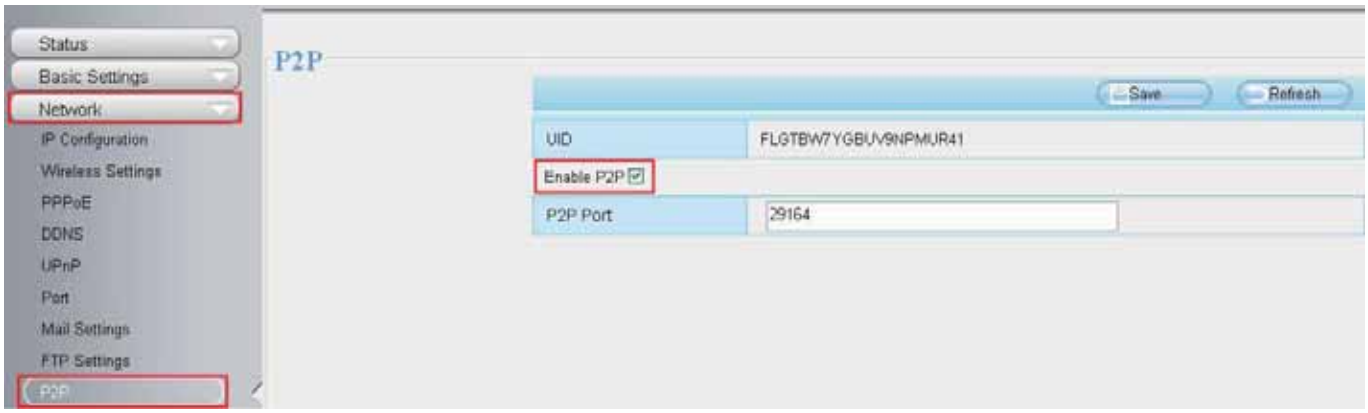


Figure 4.46

Search and install **Foscam Viewer** on Google Play and App Store for for Android and iOS devices.
If you want to know more details of the iOS APP or Android APP, see the *iOS App User Manual* or *Android App User Manual*.

4.4 Video

This section allows you to configure Video stream settings, On screen display and Snapshot settings.

4.4.1 Video Settings

There are two ways to set the stream video settings. They are main stream video settings and sub stream video settings.

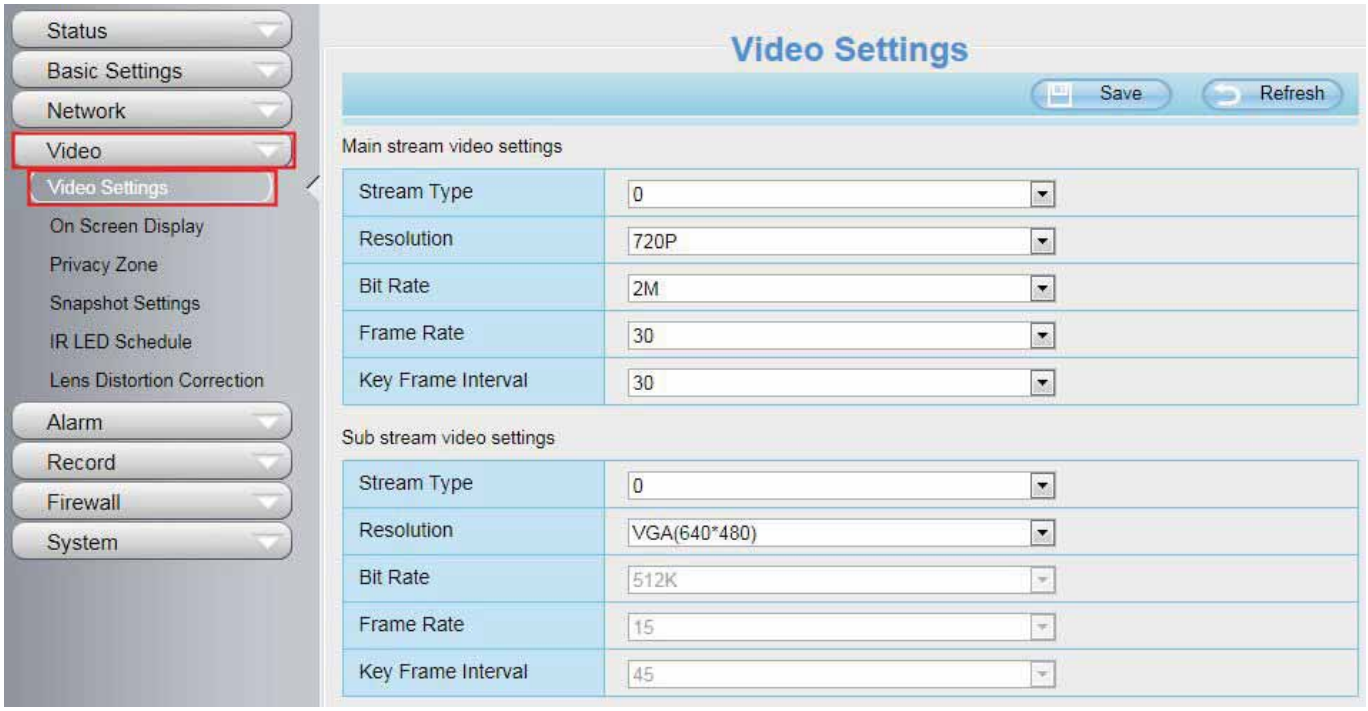


Figure 4.47

Stream type: There are four types to identify different streams you have set.

Resolution: The camera supports two types: 720P, VGA. The higher the resolution is, the clearer video will become. But the code flux will become larger too, and it will take up more bandwidth.

Bit Rate: Generally speaking, the larger the bit rate is, the clearer video will become. But the bit rate configuration should combine well with the network bandwidth. When the bandwidth is very narrow, and bit rate is large, that will lead to video can not play well.

Frame Rate: Note that a larger frame size takes up more bandwidth. When the video format is 50Hz, the maximum frame rate is 25 fps. When the video format is 60Hz, the maximum frame rate is 30 fps. You should lower frame rate when the bandwidth is limited. Normally, when the frame rate above 15, you can achieve fluently video.

Key Frame Interval: The time between last key frame and next key frame. The shorter the duration, the more likely you will get a better video quality, but at the cost of higher network bandwidth consumption.

4.4.2 On Screen Display

This page is used to add timestamp and device name on the video.

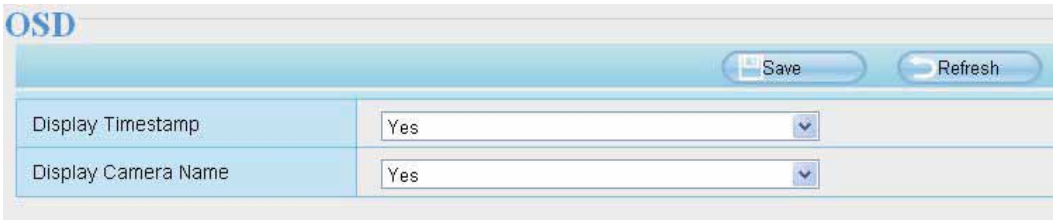


Figure 4.48

Display Timestamp: There are two options: Yes or NO. Select Yes and you can see the system date on the video,
Display Camera Name: There are two options: Yes or NO. Select Yes and you can see the device name on the video.

4.4.3 Privacy Zone

This page is used to add privacy zone on the video.

There are two options: Yes or NO. Select Yes, then click “Set Privacy Zone” and draw a privacy area on the video, the privacy area will be black on the video.

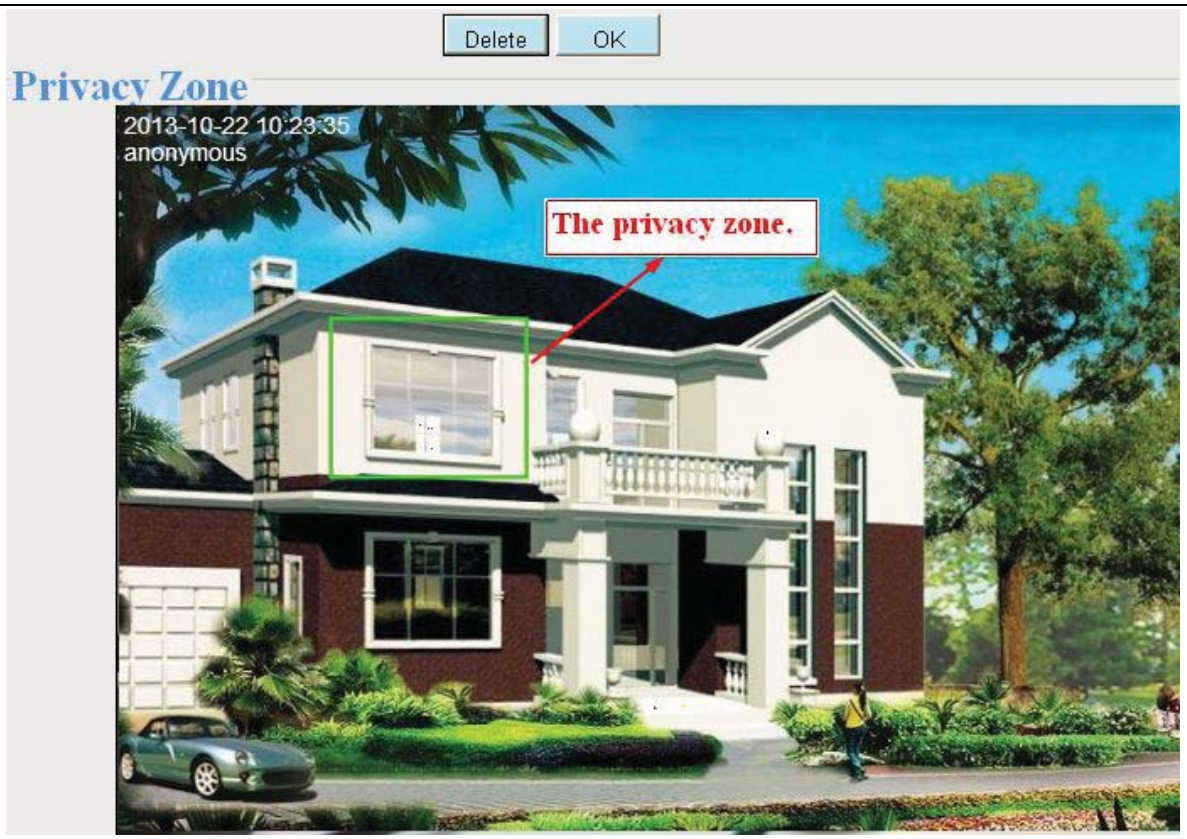


Figure 4.49

Click **OK** button and return to the **Privacy Zone** page, click Save to take effect.
Back to the surveillance window, you can see the privacy area as the following picture:

Figure 4.50

4.4.4 Snapshot Settings

On this page you can set the snapshot pictures' image quality and the storage path.

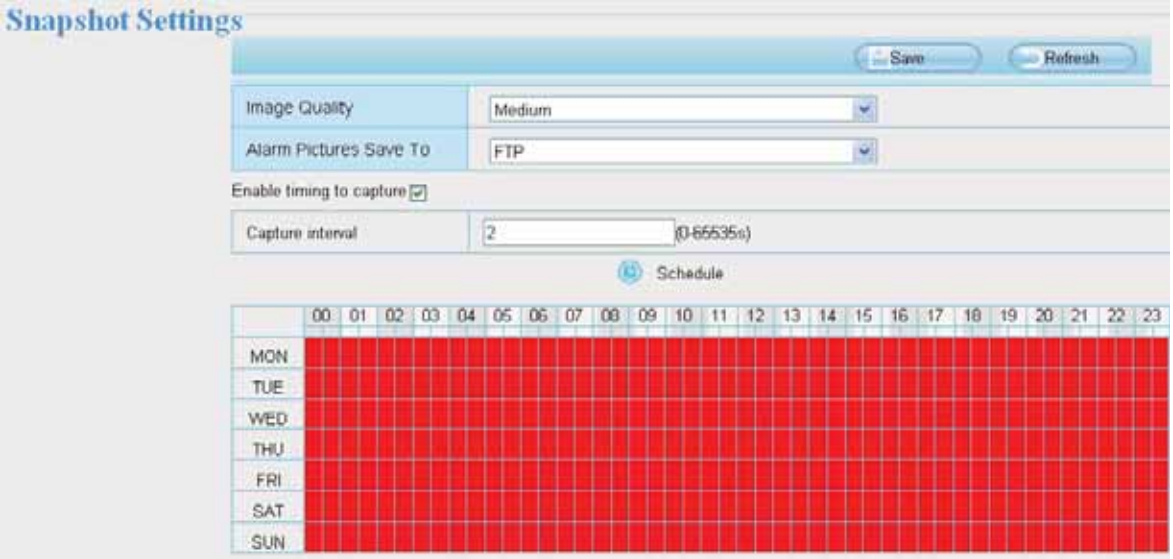


Figure 4.51

Image Quality: Low, Middle and High. The higher the quality, the picture will be clearer.
Alarm Pictures Save Path: FTP. If you have done FTP and Alarm settings, when alarming, the camera will snap pictures to the FTP automatically.
Enable timing to capture
To enable capture interval, follow the steps below:
1 Select **Enable timing to capture**
2 Capture interval: The interval time between two captures.
3 Select the capture time

- Capture anytime
  Click the black button up the MON, you will see all time range turn red. When something moving in the detection area at anytime, the camera will capture.
- Specify an capture schedule
  Click the week day words, the corresponding column will be selected. For example, click TUE, the all column of TUE turns to red, that means during Tuesday whole day, the camera will capture.
- Press the left mouse and drag it on the time boxes, you can select the serial area,

4 Click **Save** button to take effect.

4.4.5 IR LED Schedule

You can set the period of time during which the infrared lamp is turned off to prevent your baby from being influenced during sleep. You can also turn off the infrared lamp on the video preview page at any time.

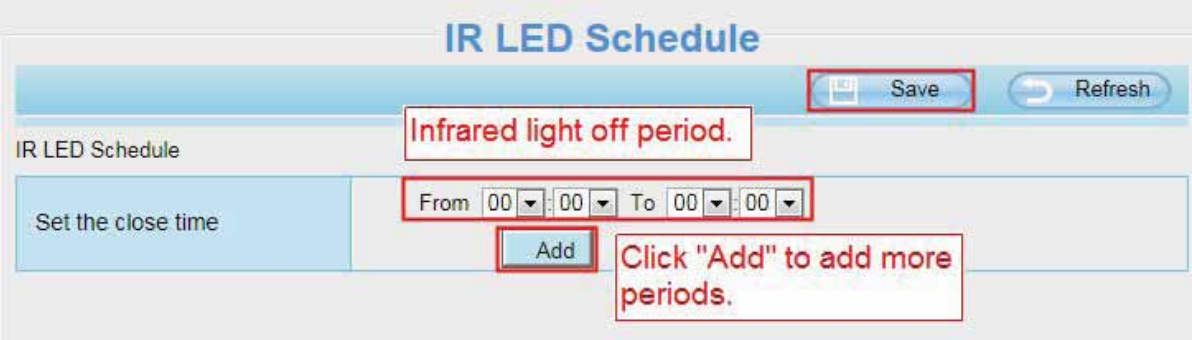


Figure 4.52

4.4.6 Lens Distortion Correction

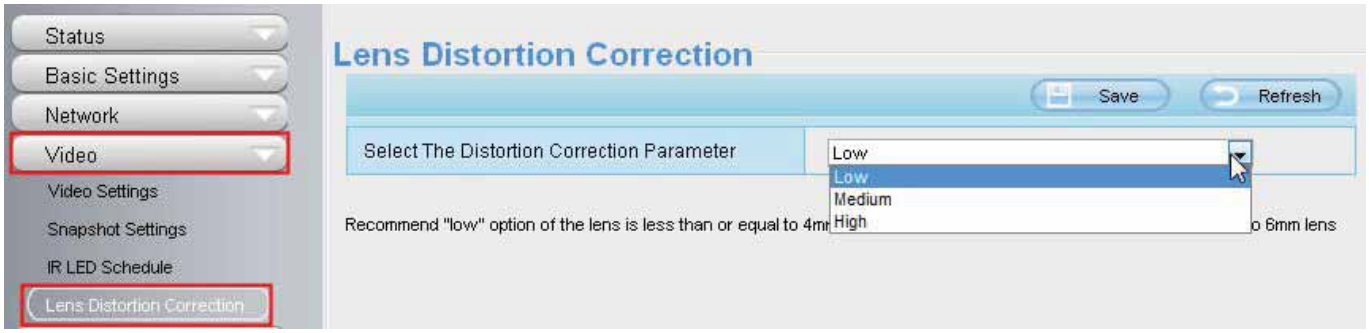


Figure 4.53

4.5 Alarm

Motion Detection

IP Camera supports **Motion Detection Alarm**, when the motion has been detected, it will send emails or upload images to FTP.

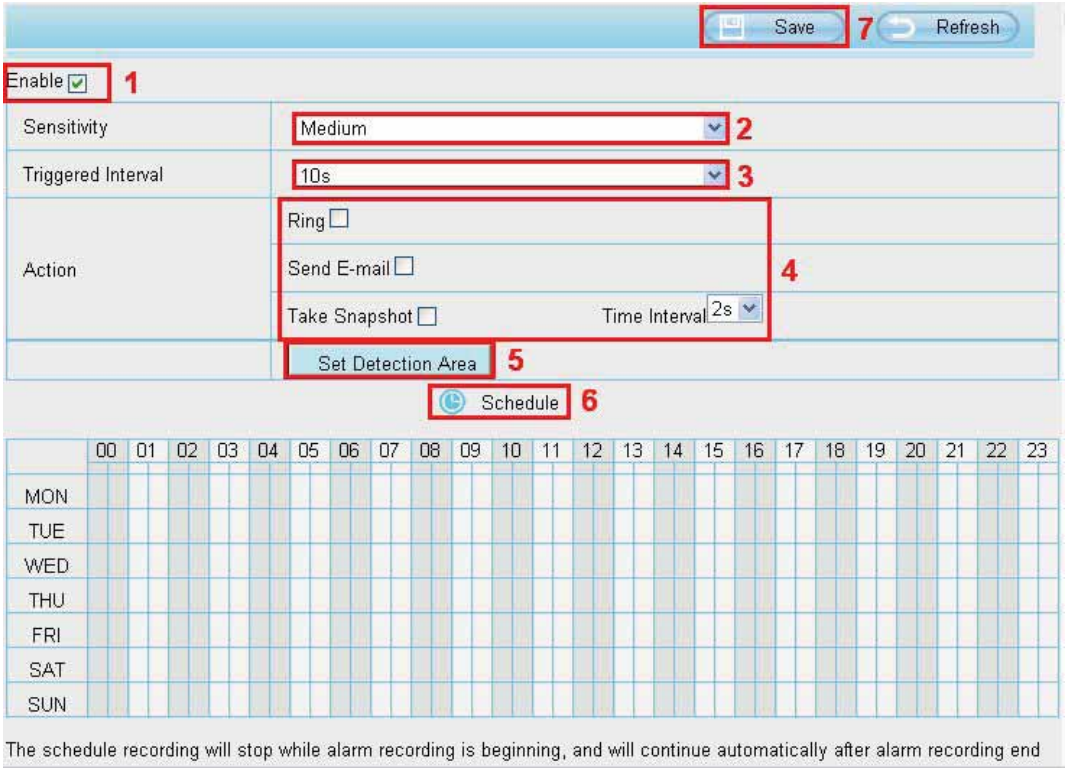


Figure 4.54

To enable motion detection, follow the steps below:

1 Enable Motion detection

2 Sensitivity---- It supports three modes: Low, Middle and High. The higher the sensitivity, the camera will be more easily alarmed. Select one motion sensitivity.

3 Trigger interval--- The interval time between two motion detections. Here supports 5s/6s/7s/8s/9s/10s/11s/12s/13s/14s/15s. Select one interval time.

4 Select the alarm indicators

When the motion has been detected, the alarm status will turn to Detect alarm.

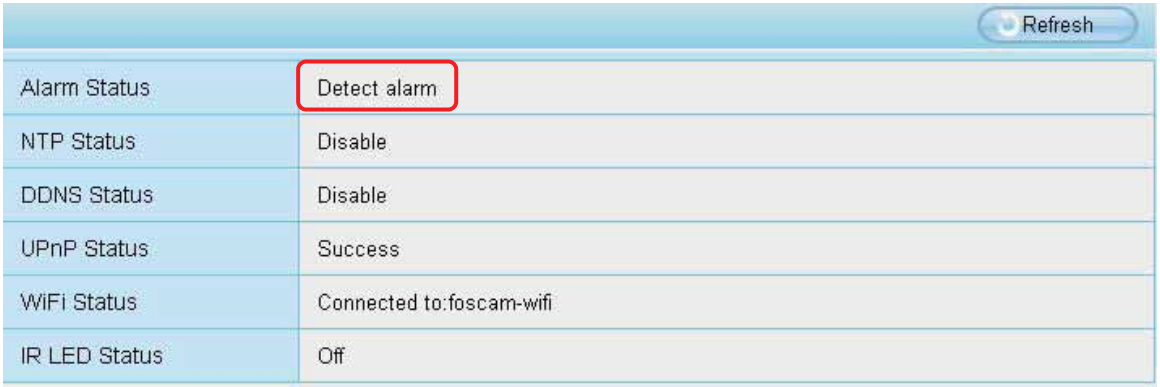


Figure 4.55

There are three alarm indicators:

A Ring

If the camera has connected with a speaker or other audio output device, if you select Ring, when the motion

has been detected, the people around the camera will hear beep alarm sound.

B Send Mail

If you want to receive alarm emails when motion is detected, you must select Send Mail and set Mail Settings first. The alarm email cannot contain the alarm picture if you have not selected **Snap picture**.

C Snap picture

If you select this checkbox, when the motion has been detected, the camera will snap the live view window as a still picture and load it to the FTP. If you select Send Email, at the same time the picture will be send to you as an attachment. Make sure you have set FTP and set FTP as the storage path in Video->Snapshot Settings panel.

Time interval: The interval time between two pictures.

5 Set Detection Area

Click set Detection Area and it pop up a window, then you can draw the detection area. Click **OK** button after settings. When something moving in the detection area, the camera will alarm.

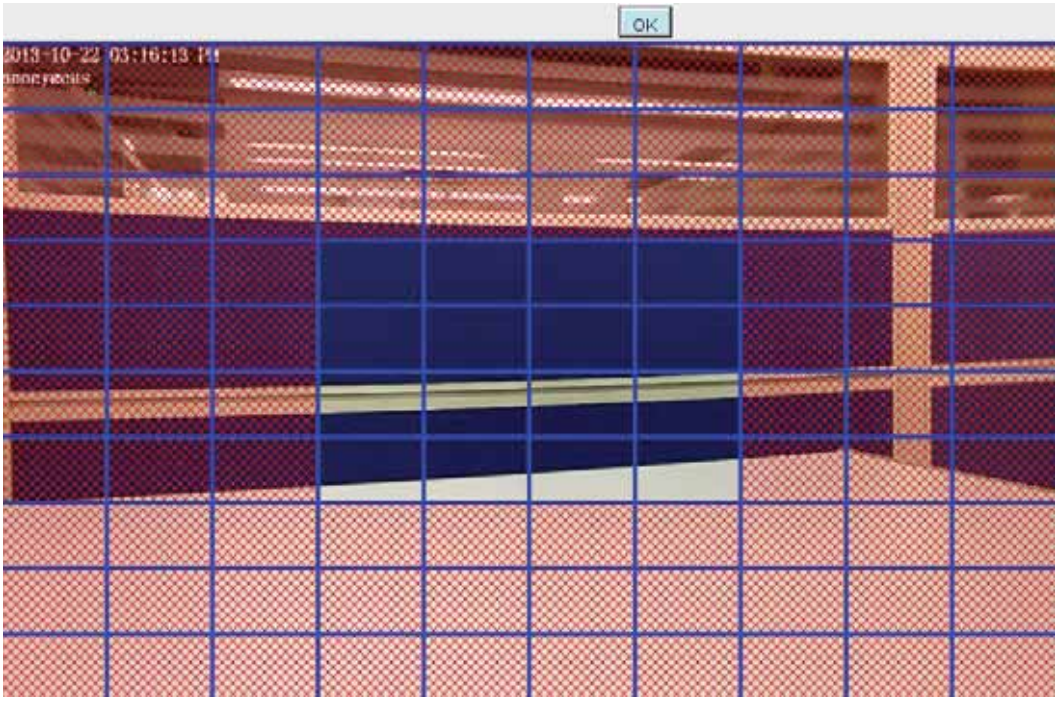


Figure 4.56

6 Alarm Schedule

① Alarm anytime when motion is detected

Click the black button up the MON, you will see all time range turn red. When something moving in the detection area at anytime, the camera will alarm.

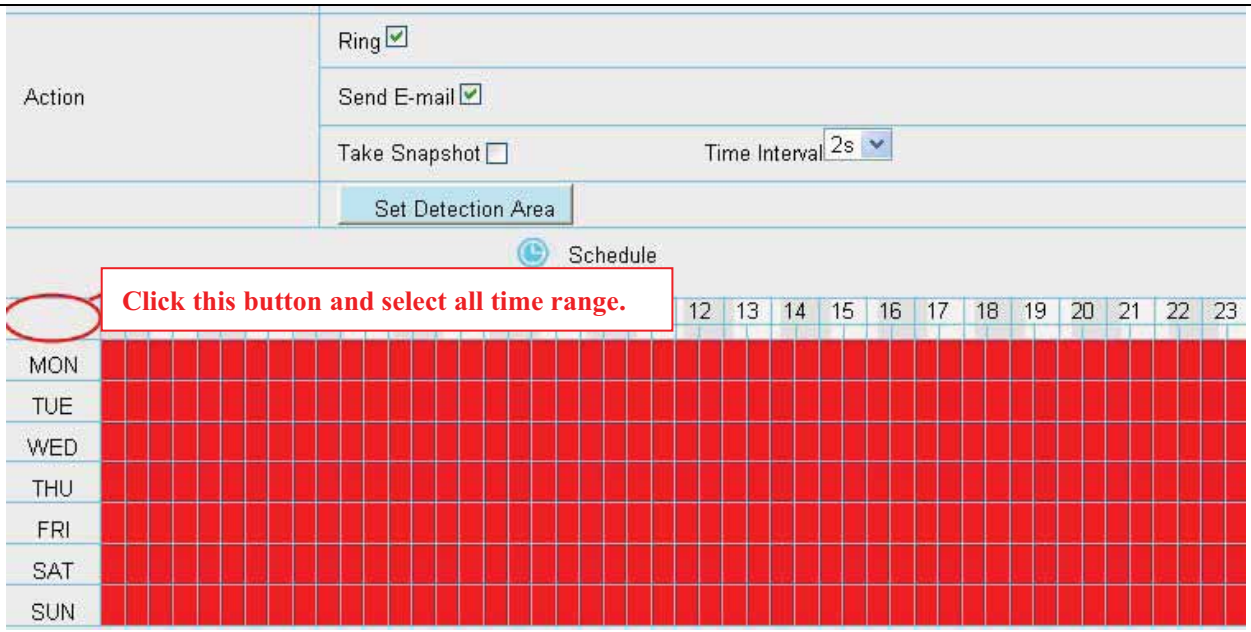


Figure 4.57

② Specify an alarm schedule

Click the week day words, the corresponding column will be selected. For example, click TUE, the all column of TUE turns to red, that means during Tuesday whole day, when something moving in the detection area, the camera will alarm.

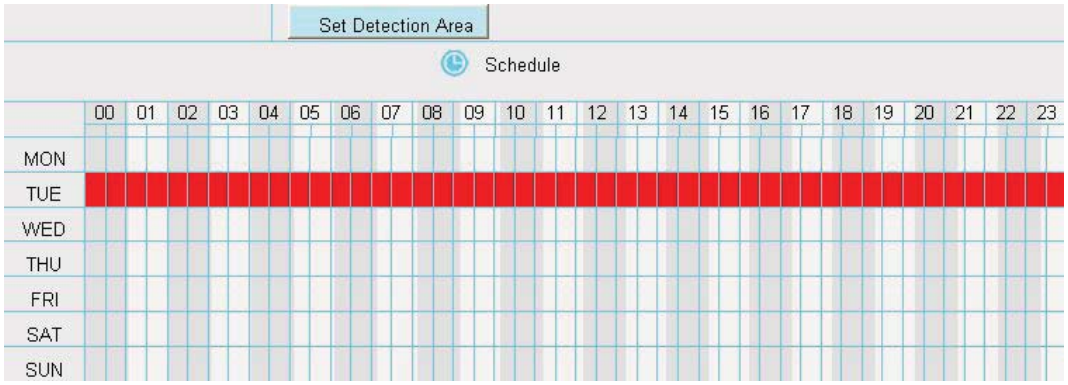


Figure 4.58

③ Press the left mouse and drag it on the time boxes, you can select the serial area,

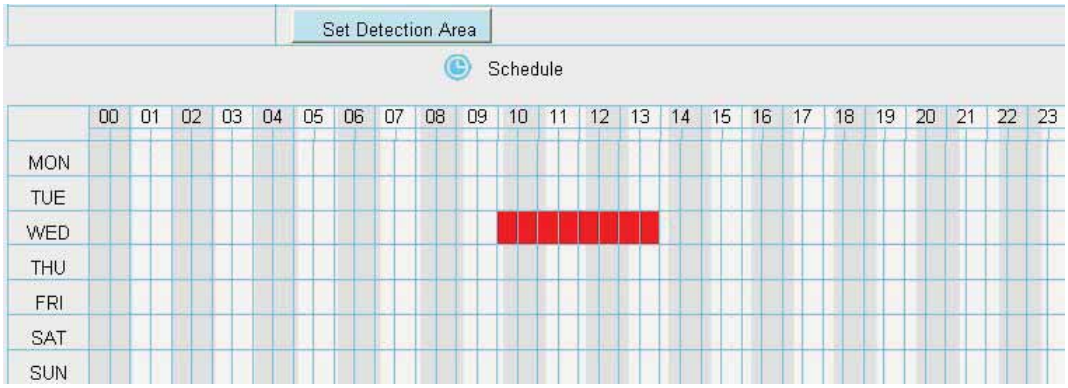


Figure 4.59

7 Click Save button to take effect. When the motion is detected during the detection time in the detection area, the camera will alarm and adopt the corresponding alarm indicators.

NOTE: You must set the detection area and detection schedule, or else there is no alarm anywhere and anytime.

4.6 Record

4.6.1 Storage Location

On this page you can change the manually recording storage path, the default storage path is c:\IPCamRecord.

Figure 4.60

4.6.2 Local Alarm Recording

On this page you can enable local alarm record, and select the local alarm record time.

Figure 4.61

4.6.3 Schedule Recording

On this page you can enable schedule record.

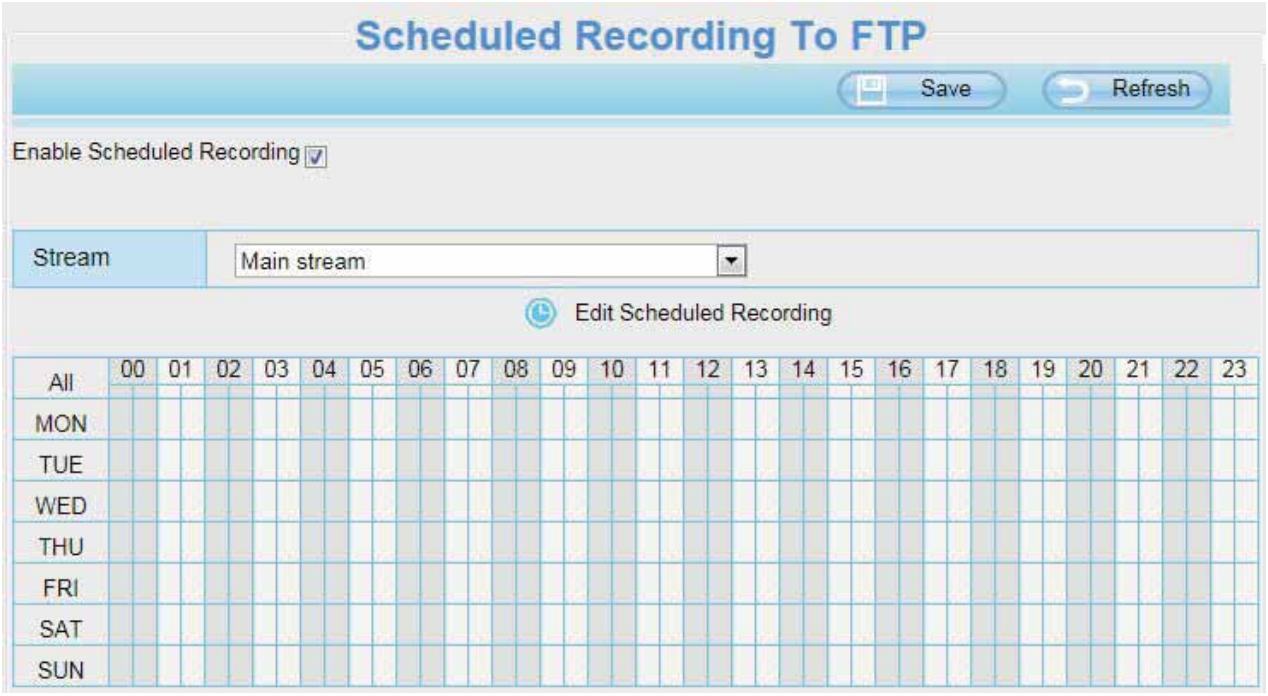


Figure 4.62

4.7 Firewall

This section explains how to control the access permission by checking the client PC's IP addresses. It is composed of the following columns: Block access from these IP addresses and Only allow access from these IP addresses.

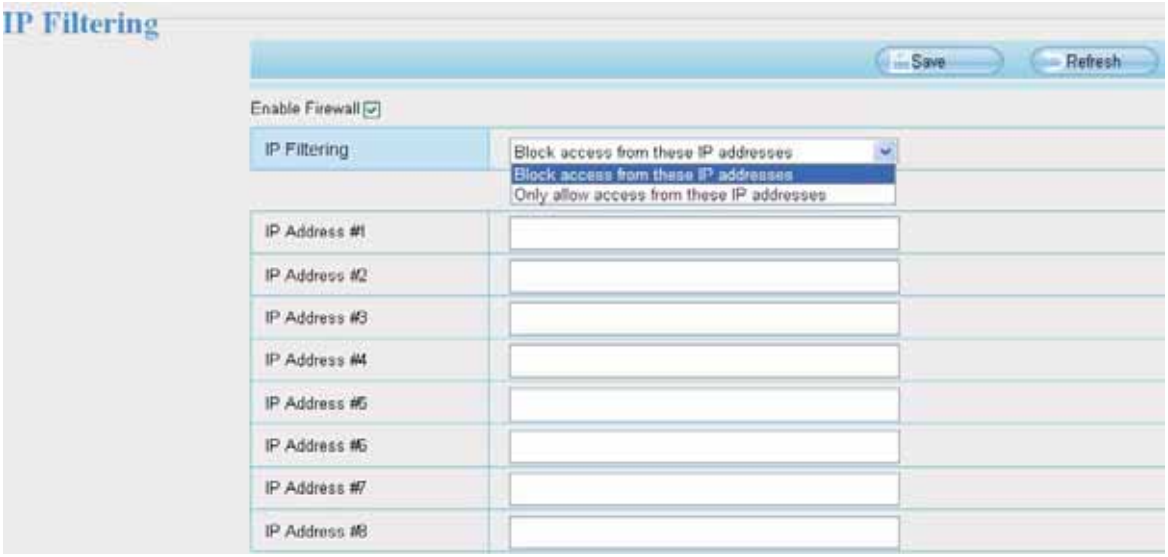


Figure 4.63

Enable firewall, If you select Only allow access from these IP addresses and fill in 8 IP addresses at most, only those clients whose IP addresses listed in the Only allow access from these IP addresses can access the Network Camera. If you select Block access from these IP addresses, only those clients whose IP addresses

are in the IP list cannot access the Network Camera.

Click **Save** to take effect.

4.8 System

In this panel, you can back up/restore your camera settings, upgrade the firmware to the latest version, restore the camera to default settings and reboot the device.

4.8.1 Back-up& Restore

Click Backup to save all the parameters you have set. These parameters will be stored in a bin file for future use.

Click Browse and select the parameters file you have stored, then click Submit to restore the restore the parameters.

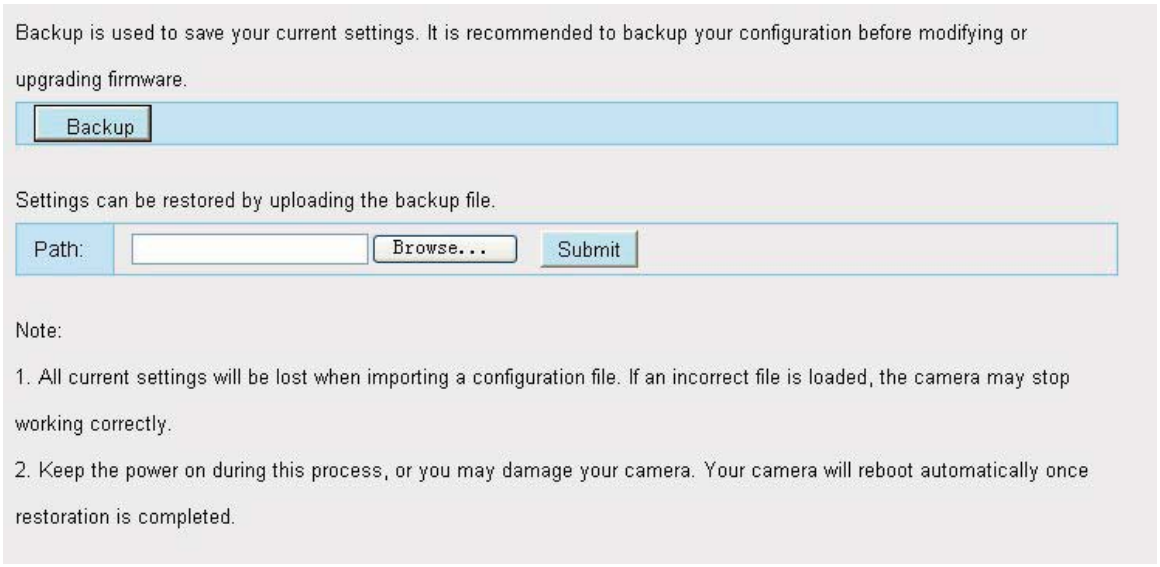


Figure 4.64

4.8.2 System Upgrade

Click Browse, choose the correct bin file(System firmware or Web UI) and then click **System upgrade**.
Don't shut down the power during upgrade. After upgrading, you can see the upgrade result.

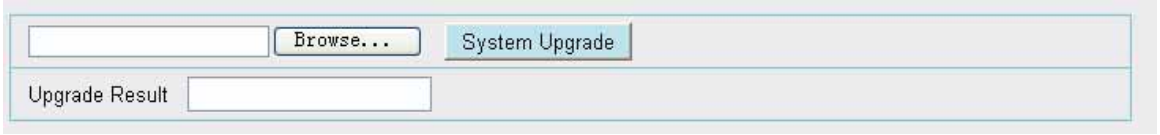


Figure 4.65

If you want to verify the firmware version of you camera, please go to Device Status-> Device Information Page to check.

Upgrade Firmware by IP Camera Tool

Double click the IP Camera Tool shot icon , select the Camera IP that you want to upgrade the firmware. Then select Upgrade Firmware and enter the username and password, choose the firmware file, and upgrade.

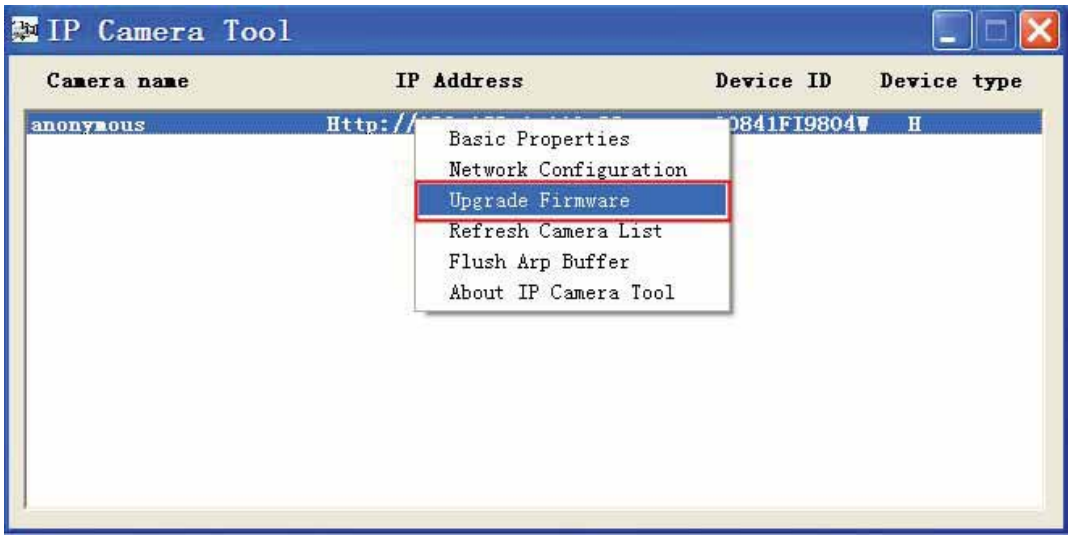


Figure 4.66

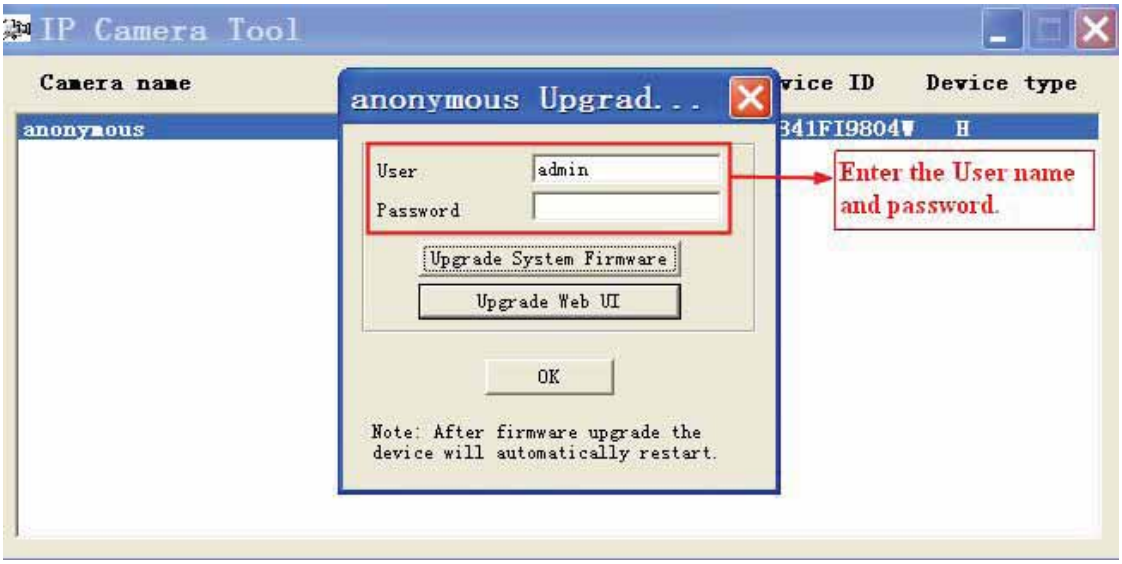


Figure 4.67

CAUTION: If your camera works well with the current firmware, we recommend not upgrading. Please don't upgrade the firmware unnecessarily. Your camera may be damaged if misconfigured during an upgrade.

NOTE:

1) Don't upgrade the firmware through the web UI in WAN, or else the upgrade may be failed.

2) Please ensure you have download the correct firmware package for your camera before upgrading. Read

the upgrade documentation (readme.txt file) in the upgrade package before you upgrade.
3) Upon downloading the firmware check the sizes of the .bin files. They must match the size in the readme.txt file. If not, please download the firmware again until the sizes are the same. Your camera will not function correctly if a corrupt .bin file is used.
4) Normally, only Device WEB UI need to be upgrade, please do not try to upgrade the Device Firmware.
5) Never shut down the power of the camera during upgrade until the IP camera restart and get connected.
6) After upgrade successfully, please clear the cache of browser, uninstall the old plugin and re-install it, then reset the camera to the default factory settings before using the camera.

4.8.3 Factory Reset

Click **Factory Reset** button and all parameters will return to factory settings if selected.

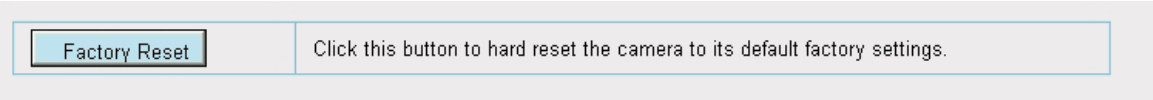


Figure 4.68

4.8.4 Reboot

Click **Reboot** to reboot the camera. This is similar to unplugging the power to the camera.

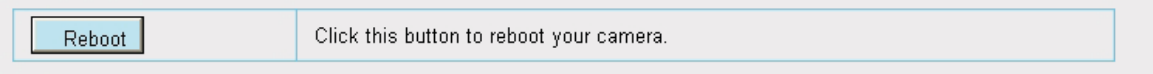


Figure 4.69

5 Appendix

5.1 Frequently Asked Questions

NOTE: Any questions you would meet, please check Network connections firstly. Check the working status revealed by the indicators on the network server, hub, exchange and network card. If abnormal, check the network connections.

5.1.1 Install / uninstall the ActiveX of Firefox browser.

5.1.1.1 Install the ActiveX of Firefox browser.

For the first time login the camera, it may prompt you to download plugin.

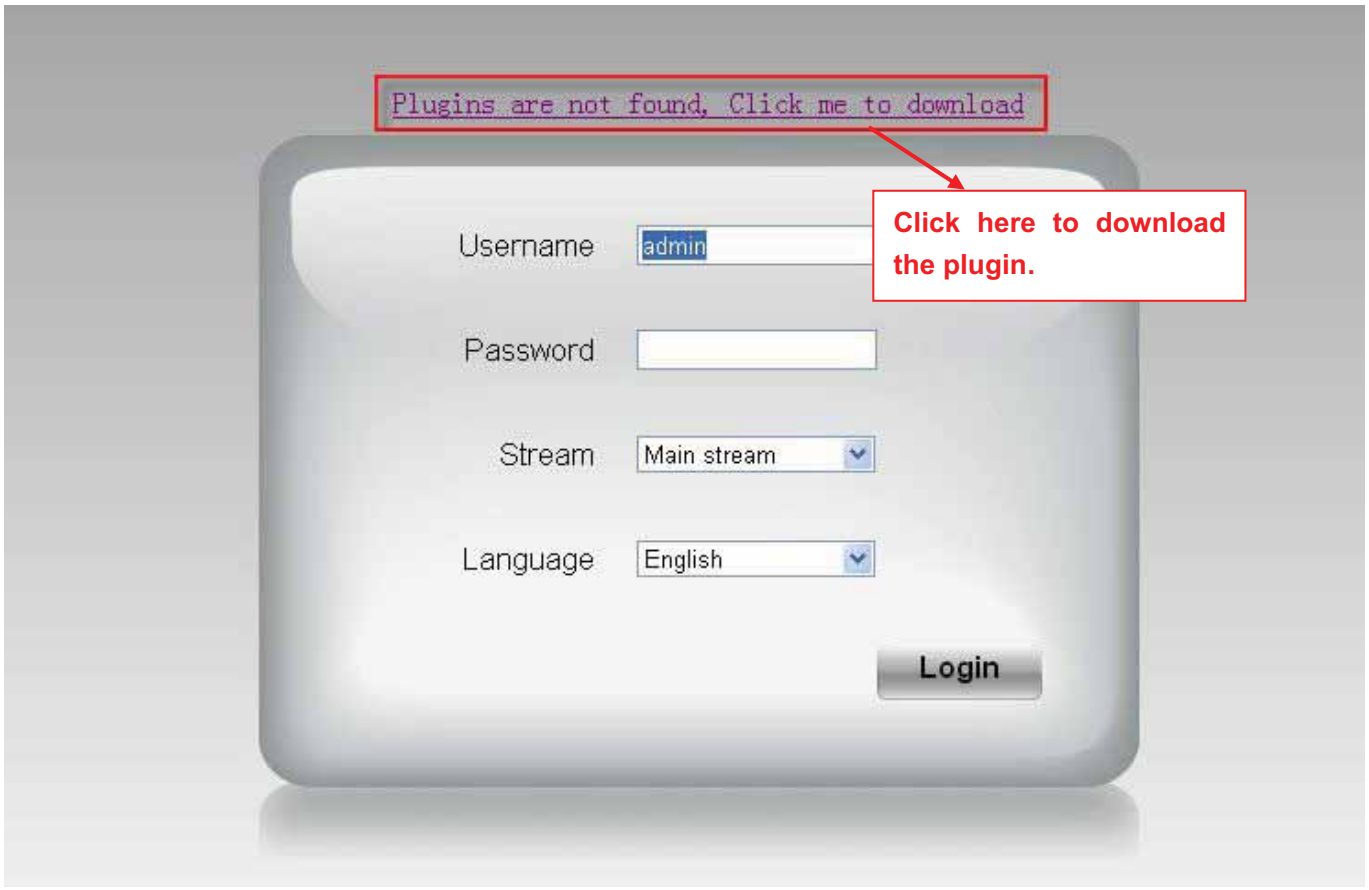


Figure 5.1

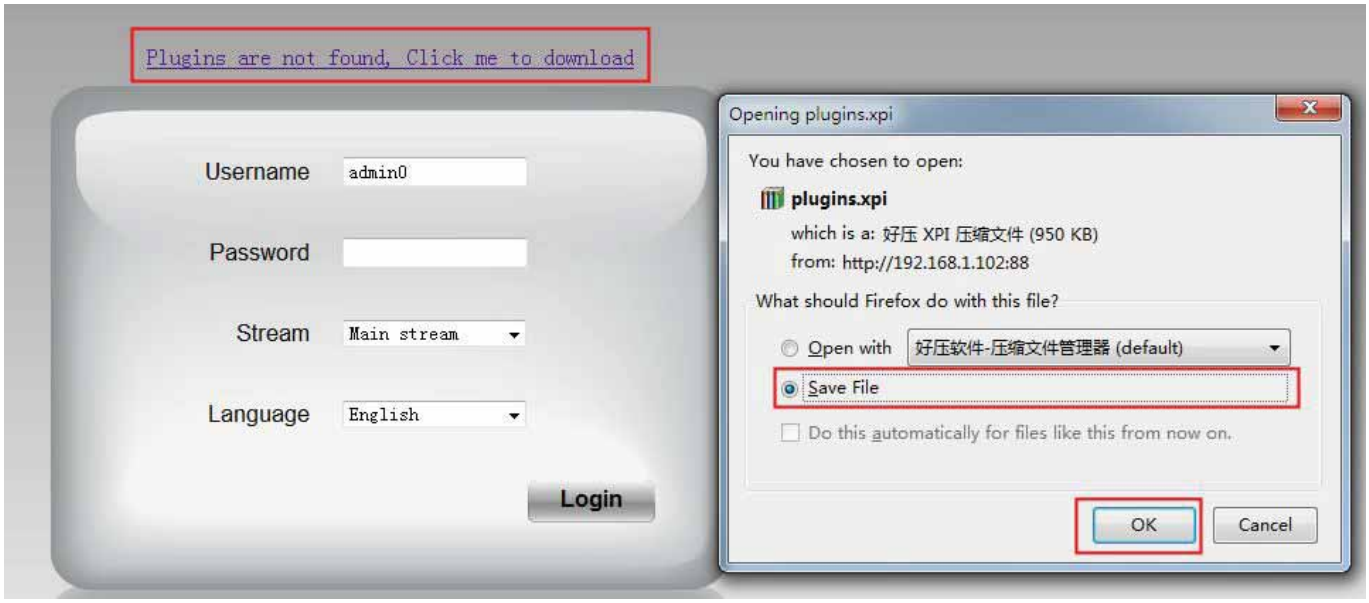


Figure 5.2

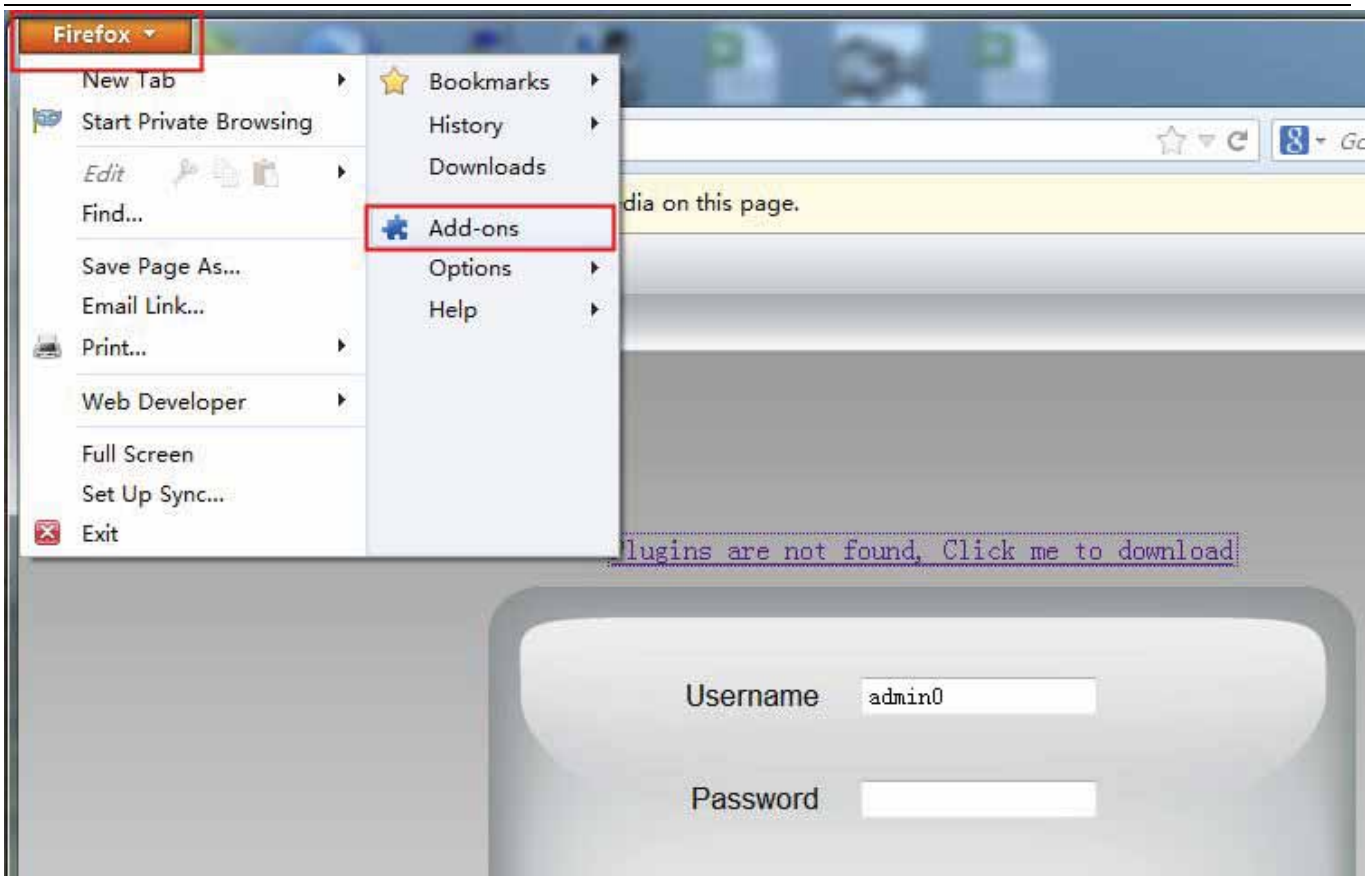


Figure 5.3

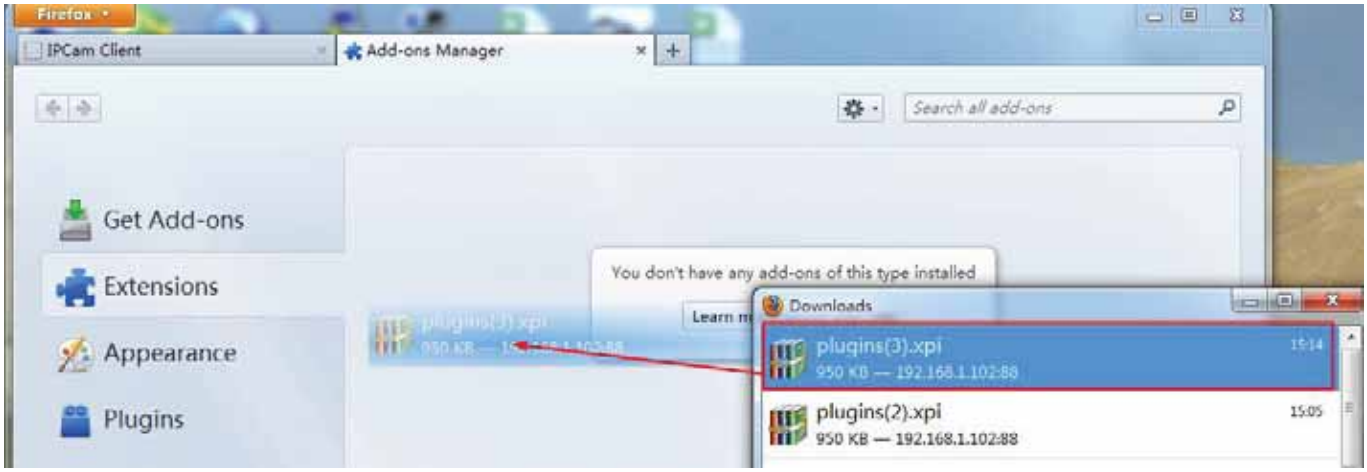


Figure 5.4

Drag the download file to Firefox web page and it will prompt you to Install it.

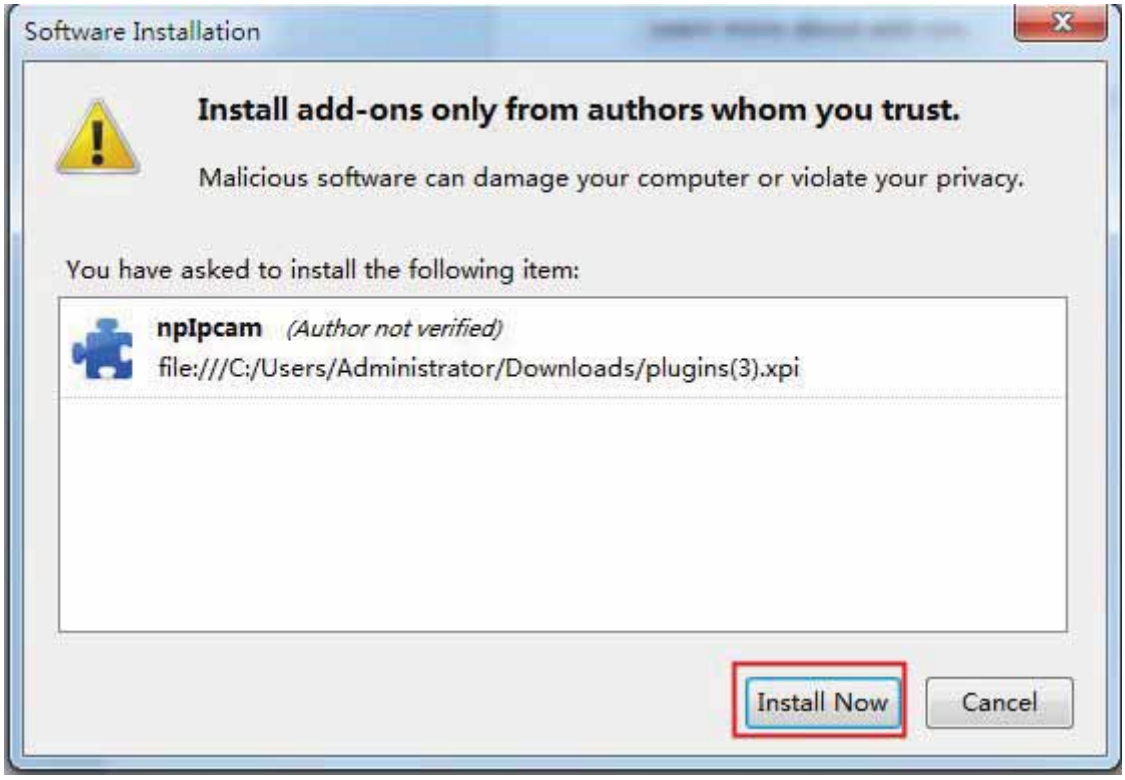


Figure 5.5

Reboot the Firefox after the plugin installation is successfully completely, then relogin the camera again, you can see the surveillance window

NOTE: If you could not view living video after running the ActiveX, only a red cross in the center of the video or just a black screen. Please change another port number to try.
Make sure all firewall or antivirus software on your computer does not block the active download and installation. If you are unable to run the ActiveX control, try shutting down the firewall or antivirus program.

5.1.1.2 Uninstall the ActiveX of Firefox browser.

After upgrading the camera's software version, in order to experience the new version better, you may need to uninstall the old ActiveX before, and then install a new one. TO uninstall the old ActiveX, you could do as follows:

1. Click on the top left of the Firefox browser menu bar, and then click "Add-ons".

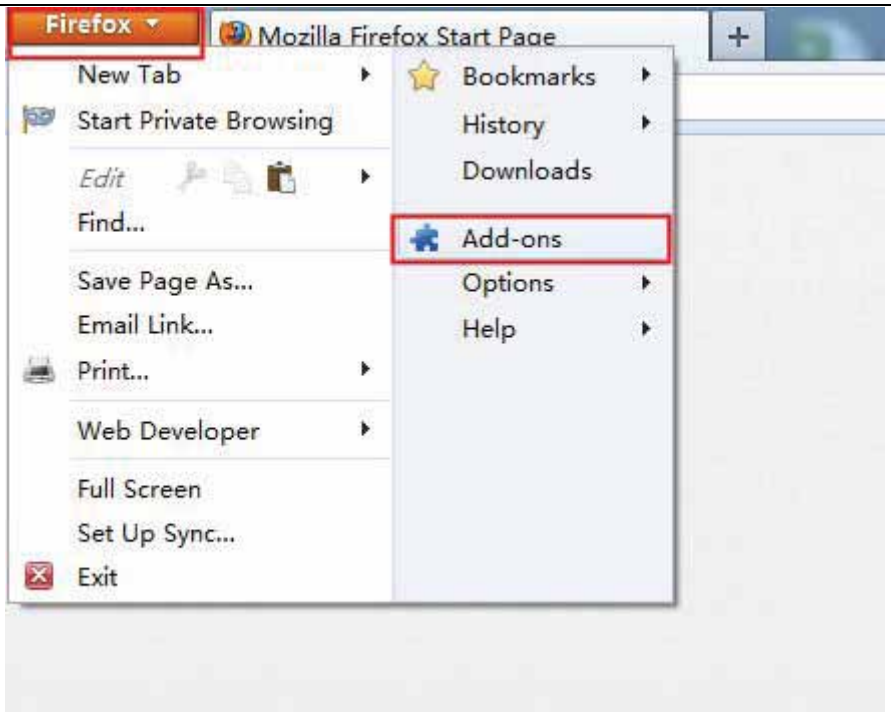


Figure 5.6

2. Click “Remove”.

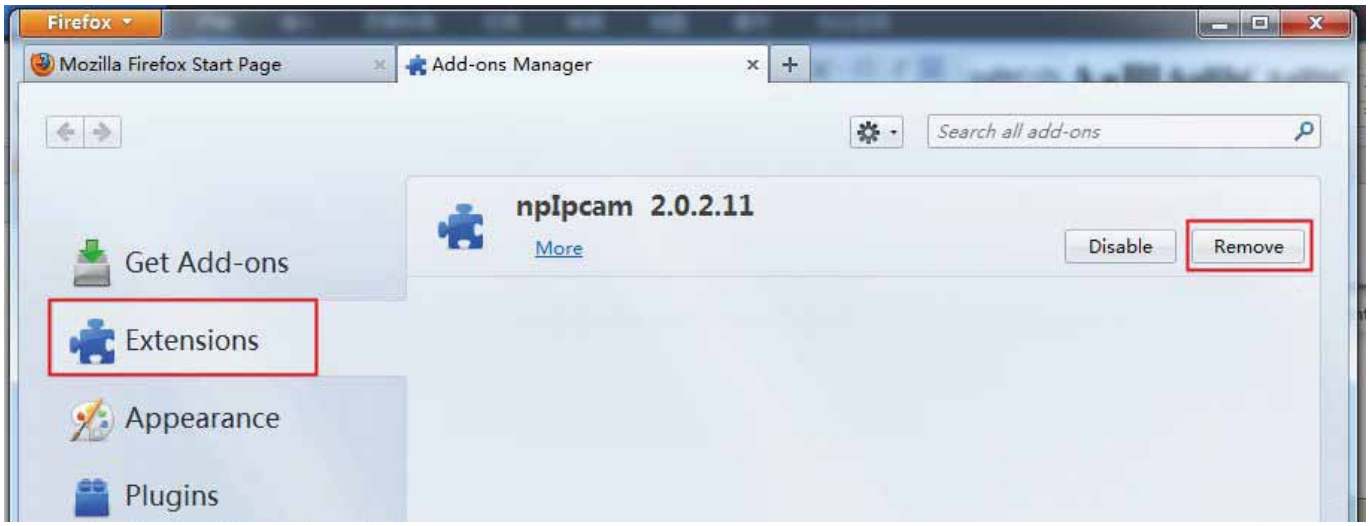


Figure 5.7

3. After the ActiveX is removed, click “Restart now”.

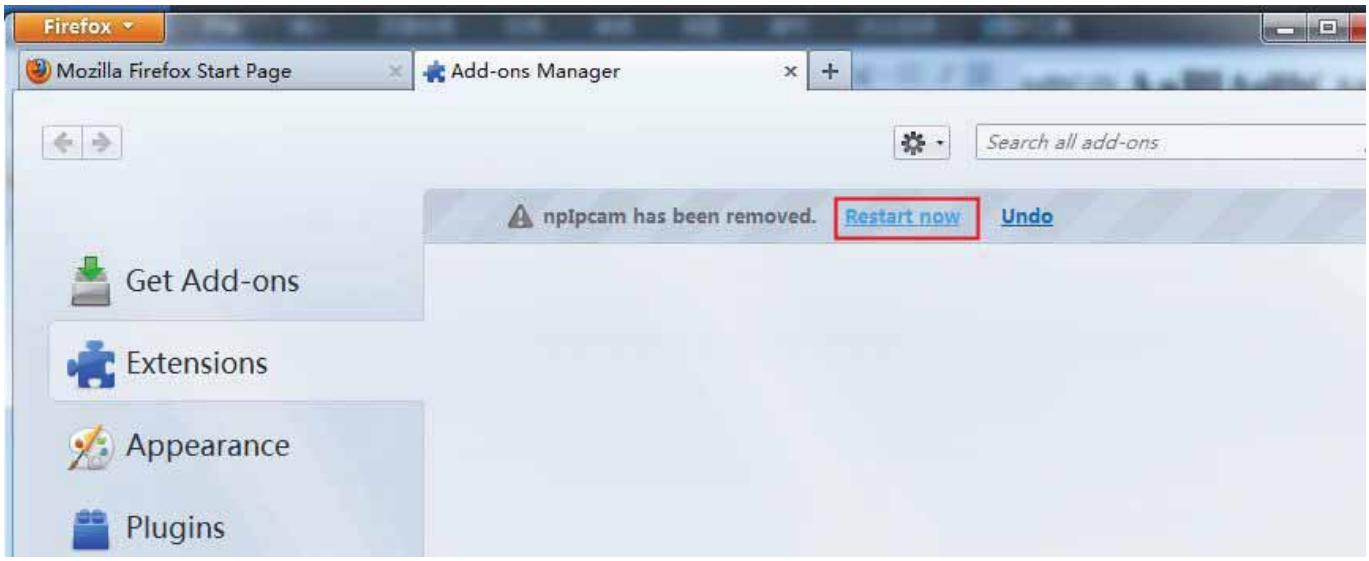


Figure 5.8

5.1.2 Install / uninstall the ActiveX of Google Chrome.

5.1.2.1 Install the ActiveX of Google Chrome.

For the first time login the camera, it will prompt you to download the ActiveX.

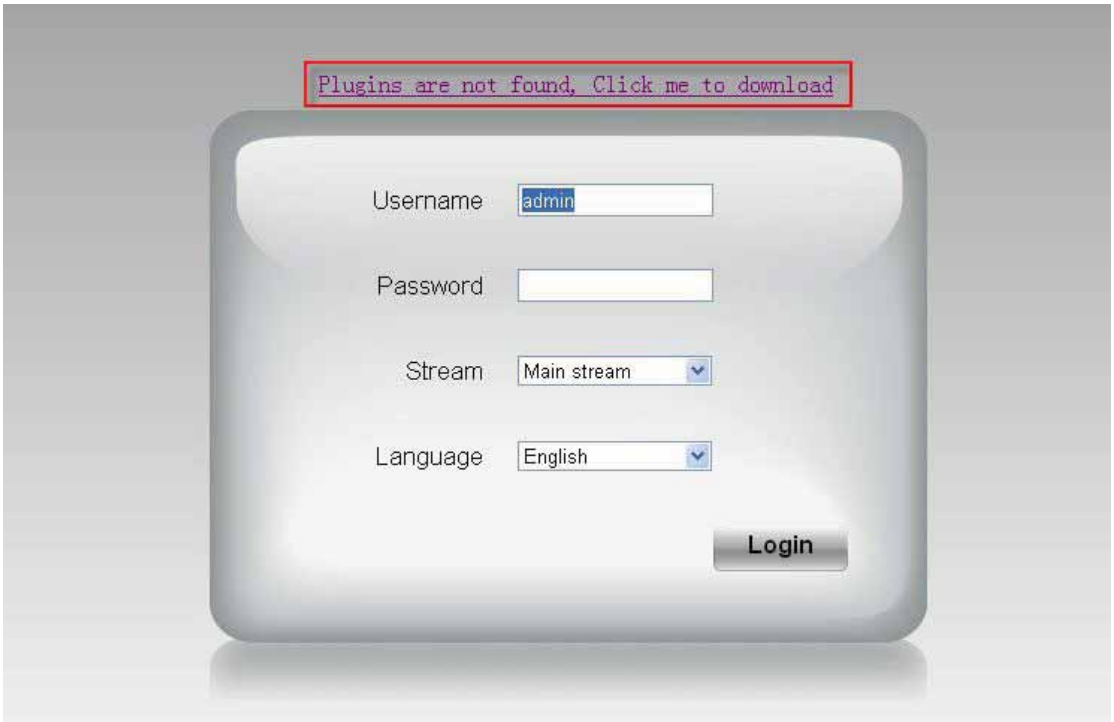


Figure 5.9

Download the plugin and drag it to the Extensions page of Google Chrome.

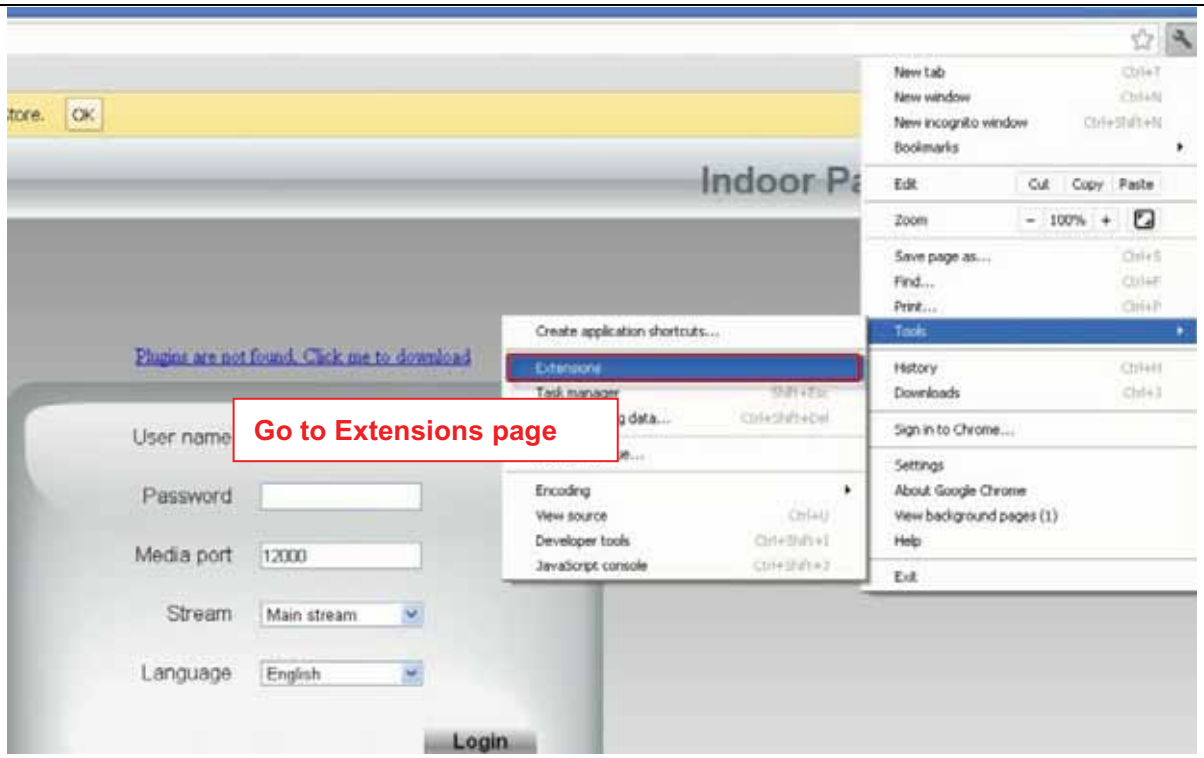


Figure 5.10

Click Add button to install the Plugins.

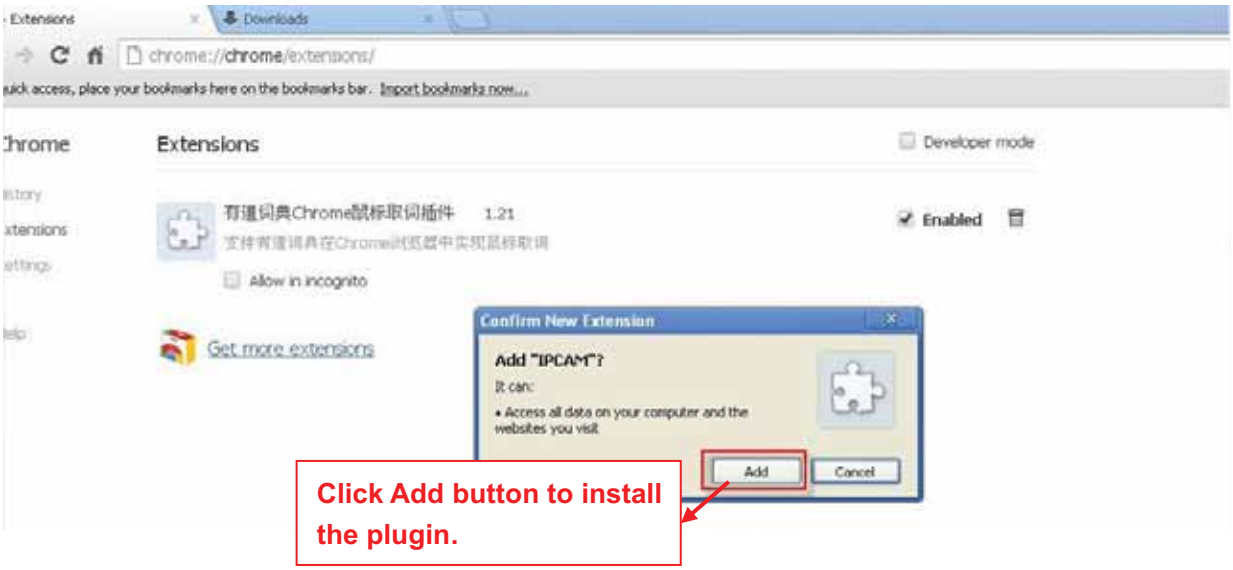


Figure 5.11

Reboot the browser and login the camera again, you will see the surveillance window.

5.1.2.2 Uninstall the ActiveX of Google Chrome.

After upgrading the camera's software version, in order to experience the new version better, you may need to uninstall the old ActiveX before, and then install a new one. TO uninstall the old ActiveX, you could do as follows:

5. Click on the top right corner of the Google browser menu bar, it will pop-up the drop-down menu, then click "Tools" -->"Extensions".

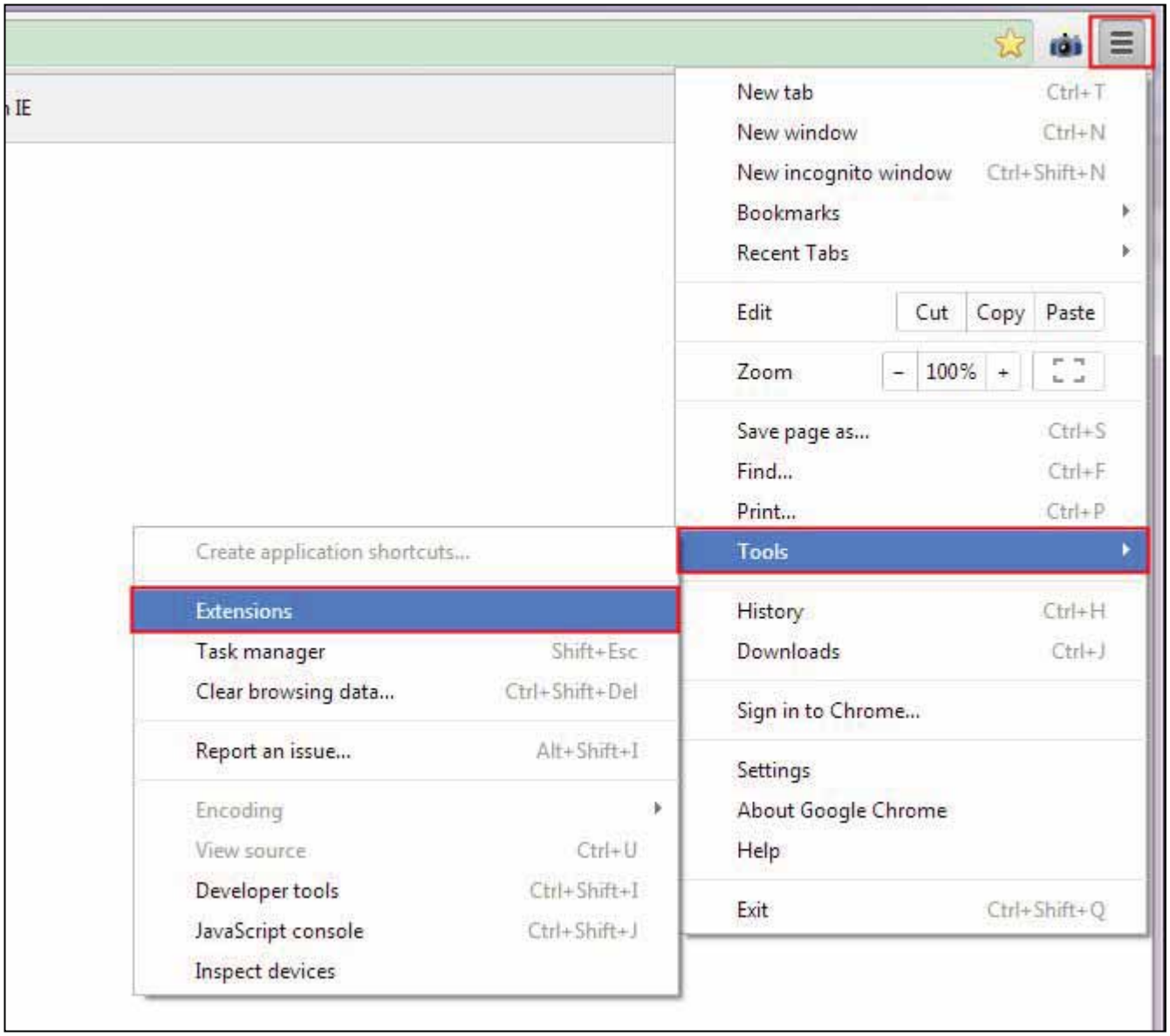


Figure 5.12

2. Select " IPCAM ", and click the trash canon on the right side.

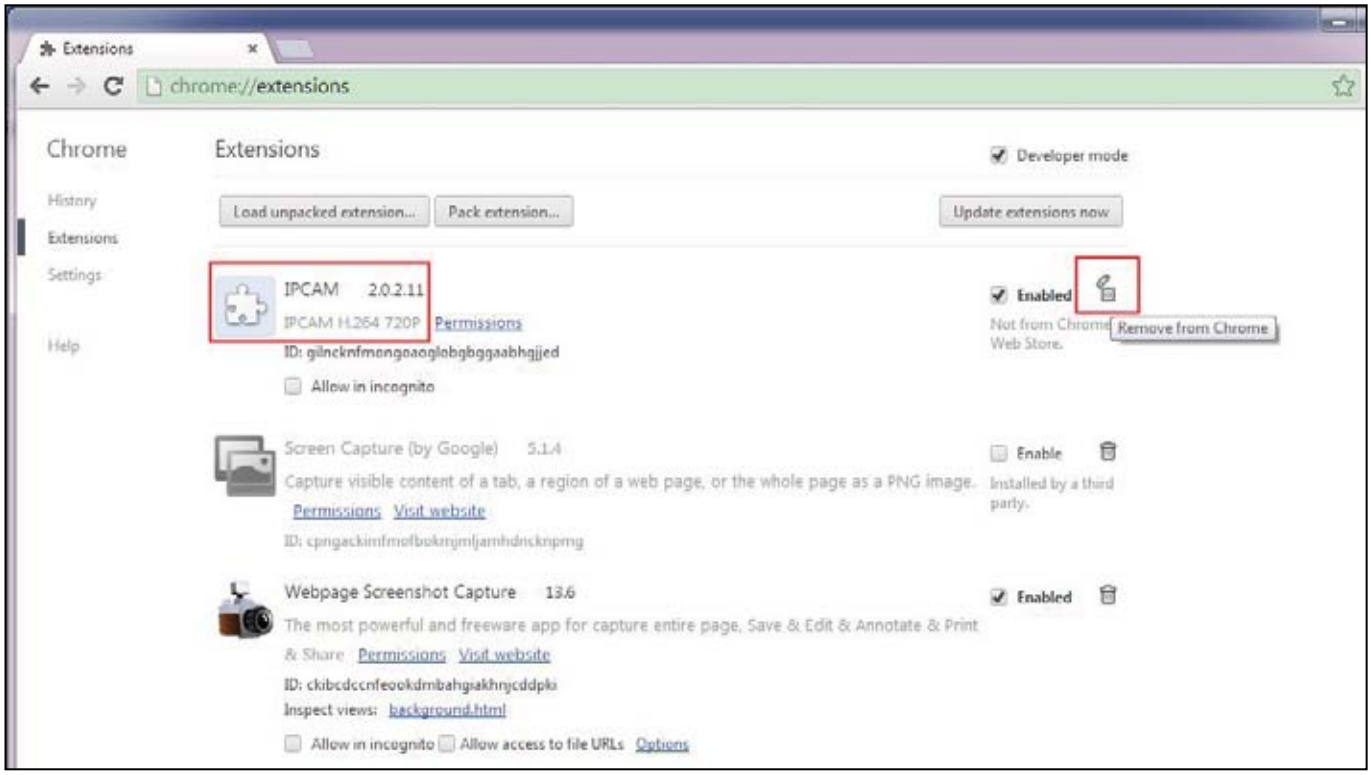


Figure 5.13

3. Click “Remove”, then restart the browser.

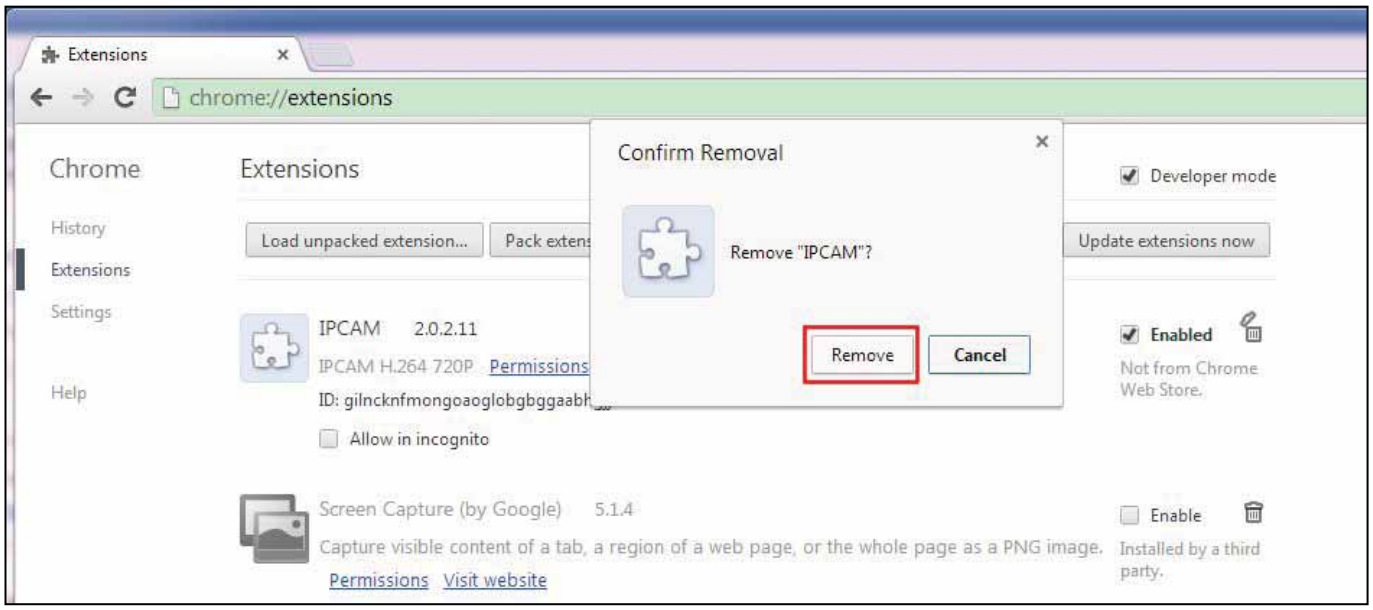


Figure 5.14

5.1.3 Install / Uninstall the ActiveX of IE Browser.

When logging in for the first time, you need to download and install the ActiveX add-on.

5.1.3.1 Install the ActiveX of IE browser.

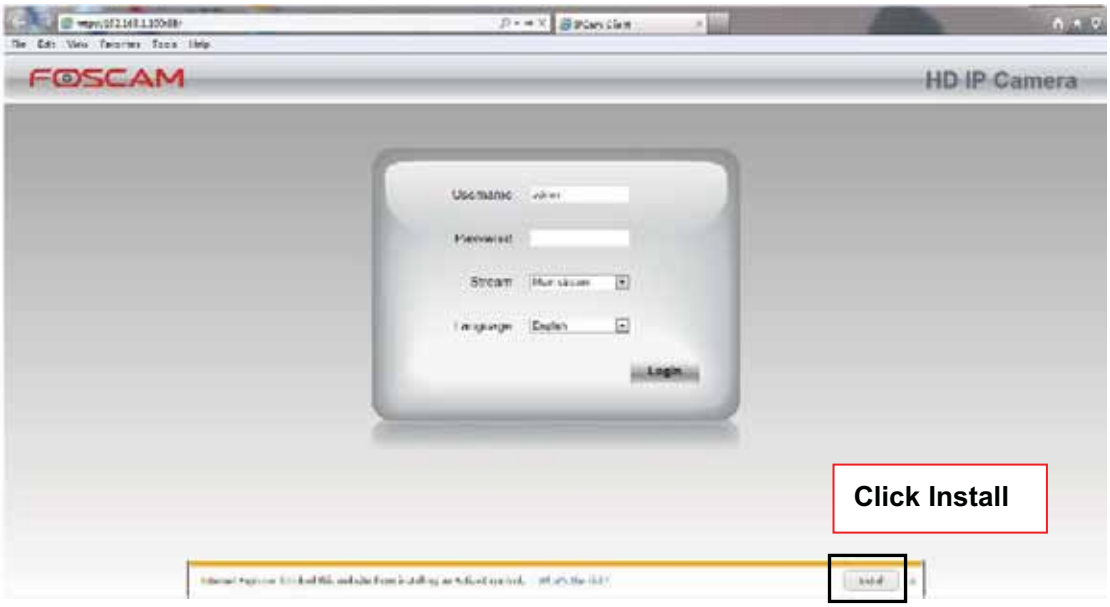


Figure 5.15

5.1.3.2 Uninstall the ActiveX of IE browser.

After upgrading the camera's software version, in order to experience the new version better, you may need to uninstall the old ActiveX before, and then install a new one. TO uninstall the old ActiveX, you could do as follows:

1. Close the IE browser, and then re-open it, making sure the IE does not load ActiveX (The IE browser will automatically load the ActiveX when using it to open the IPC website.)

2. Click the settings icon in the top right of the IE browser, find and click "Manage add-ons."

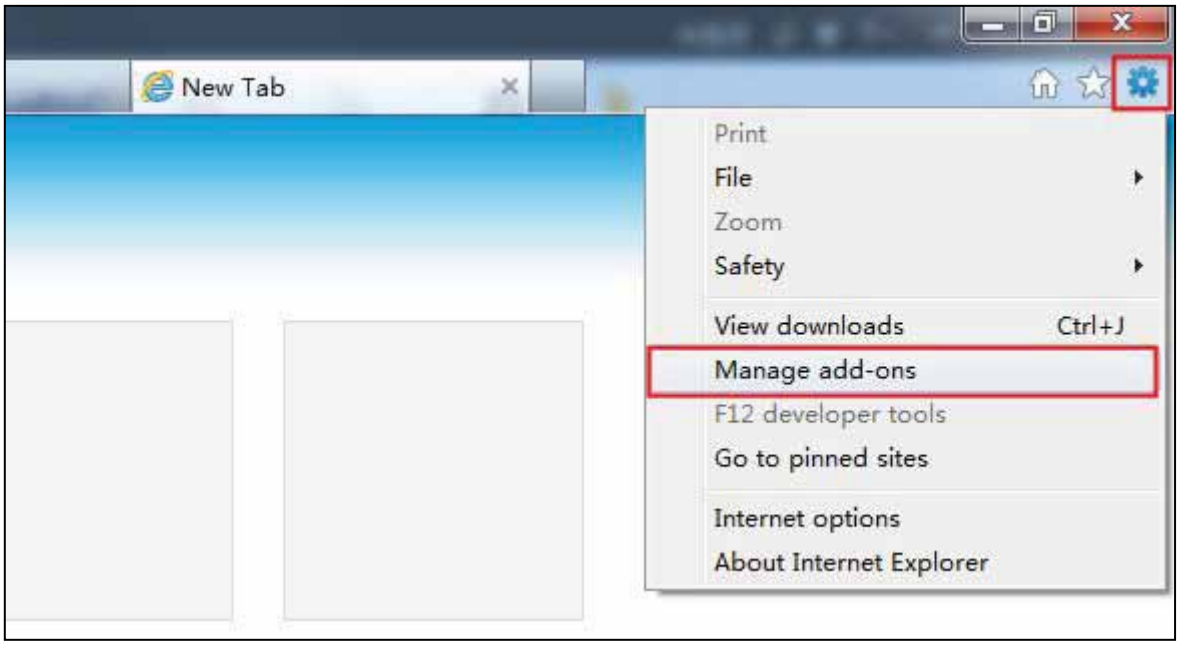


Figure 5.16

3. Click “All add-ons”.

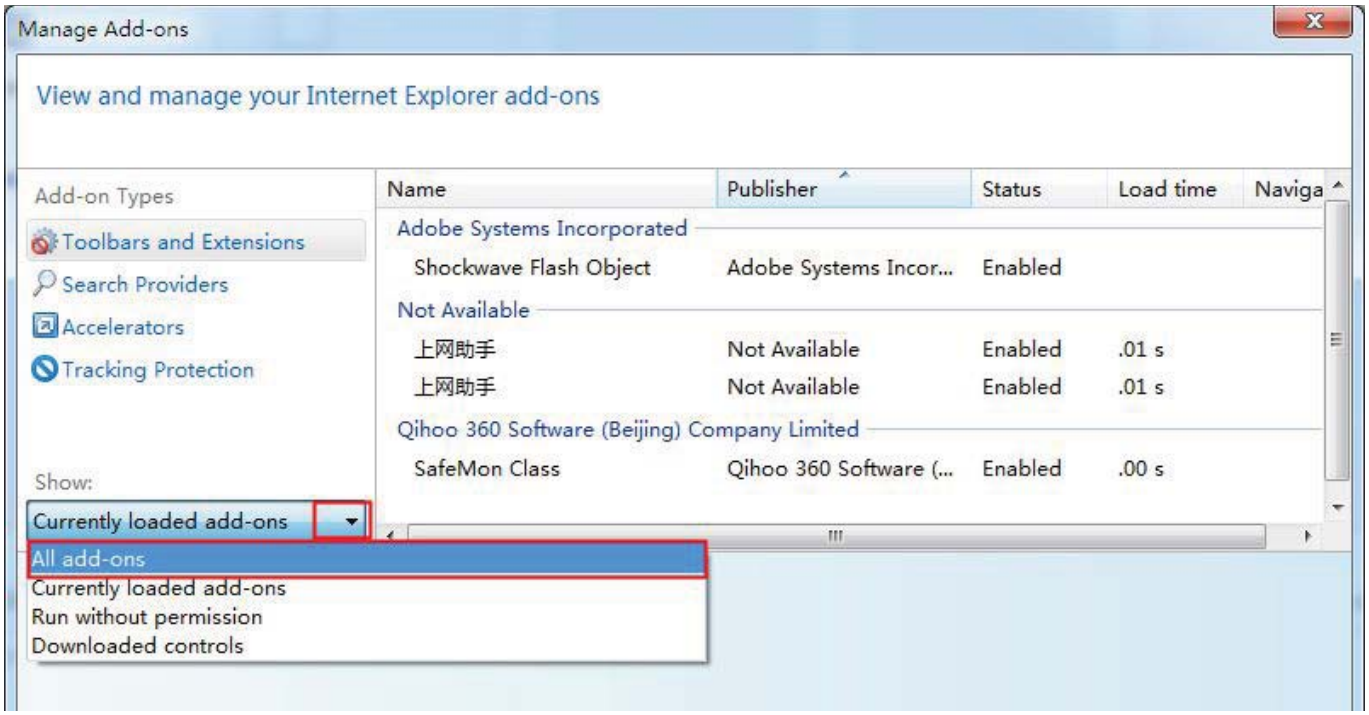


Figure 5.17

4. Click “ocxIPcam Control”, then Right-click, select “More information” (or double-click “ocxIPcam Control”).

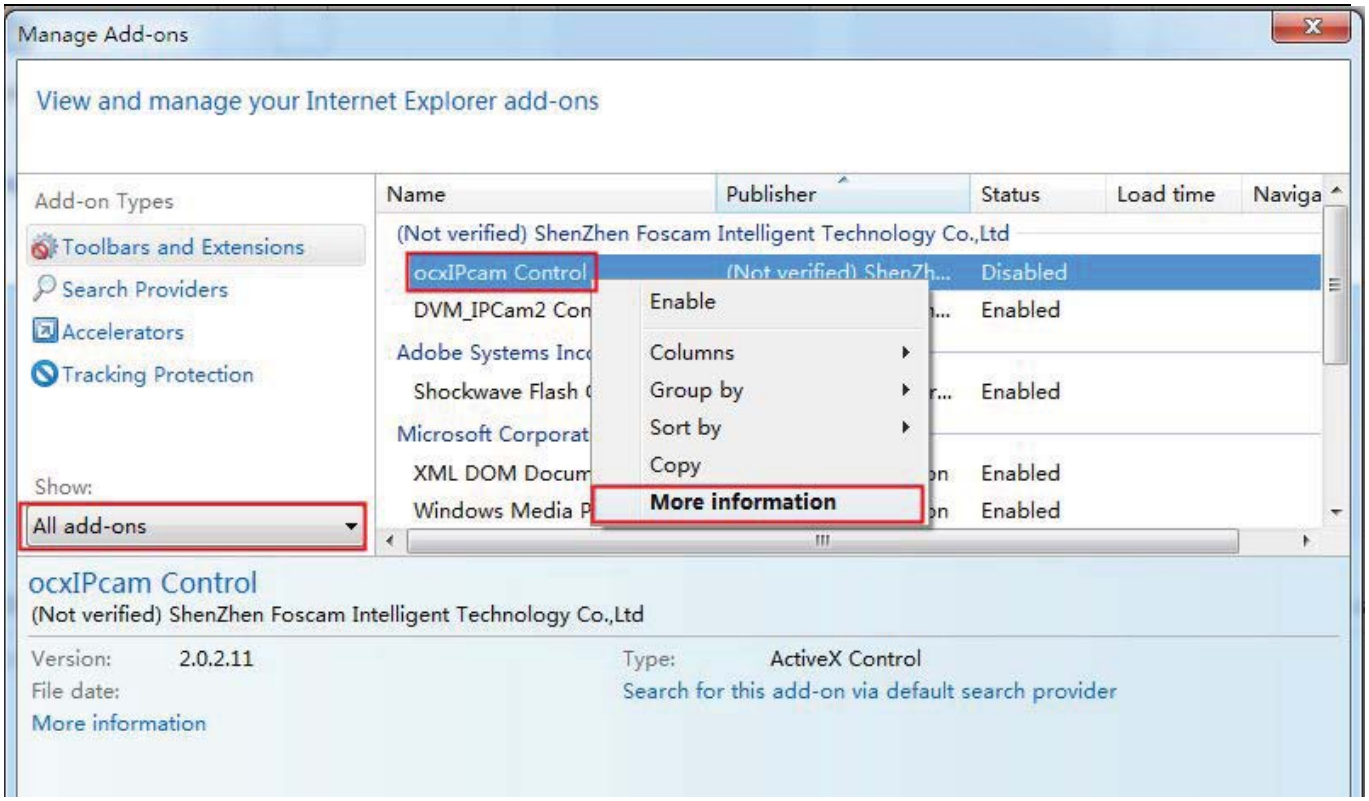


Figure 5.18

5. Click “Remove all sites—> Remove—>Close”. Then restart the IE browser.

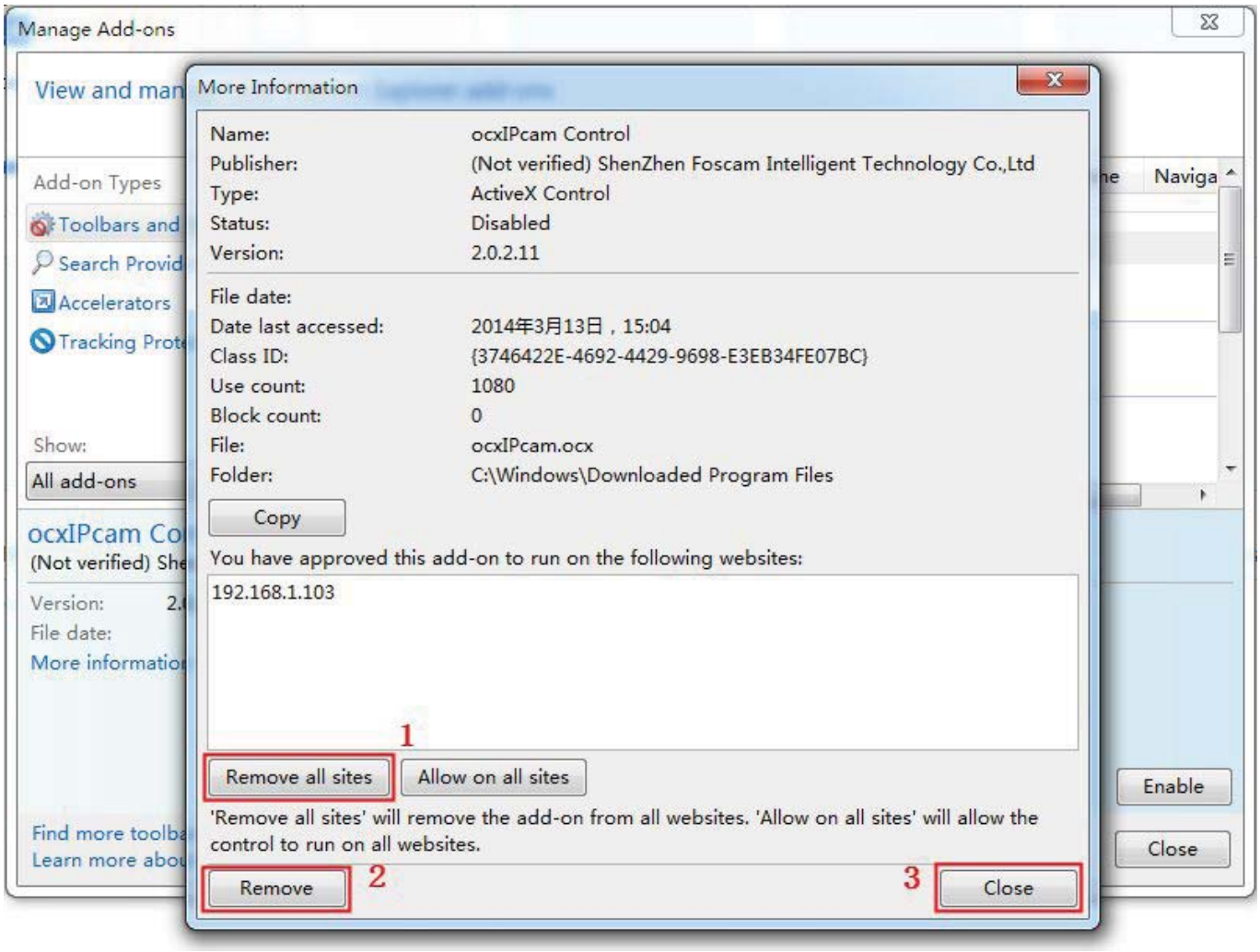


Figure 5.19

5.1.4 I have forgotten the administrator password

To reset the administrator username and password, press and hold down the RESET BUTTON for 5 seconds. Upon releasing the reset button, wait for 20 seconds, the camera will reboot and the username and password will return to the factory default administrator username and password. Please power on the camera before reset

Default administrator username: **admin**

Default administrator password: No password

5.1.5 Camera can not record

Camera can not record when I click Record button or I can't change the manually record path.

When you use Windows7 or Vista, you may be not able to do manually record or change the record path because of the security settings of computer.

There are two ways to resolve this problem:

(1) Please add the camera as a trusted site to resolve this issue. The steps are

IE browser→Tool→Internet Properties→Security→Trusted sites→Sites→Add

(2) Open IE browser, then right click, select “Run as administrator”

5.1.6 Subnet doesn’t match

Check whether your ipcamera in the same subnet of your computer. The step is Control Panel(Network Connections (Dbclick Local Area Connections (Choose General(Properties. Check subnet mask, IP address and gateways. When you set IP address please make sure they are in the same subnet. Otherwise you can't access camera.

5.1.7 No Pictures Problems

The video streaming is transmitted by the ActiveX controller. If ActiveX controller isn’t installed correctly you will see no video image. You can resolve this problem by this way:

Download ActiveX controller and set the safety property of IE in the PC when you view it first time: IE browser→Tool→Internet Proper→Security→Custom Level→ActiveX control and Plug-ins. Three options of front should be set to be “Enable”, The ActiveX programs read by the computer will be stored. As follows:

Enable: Download unsigned ActiveX controls

Enable: Initialize and script ActiveX controls not marked as safe

Enable: Run ActiveX controls and plug-ins

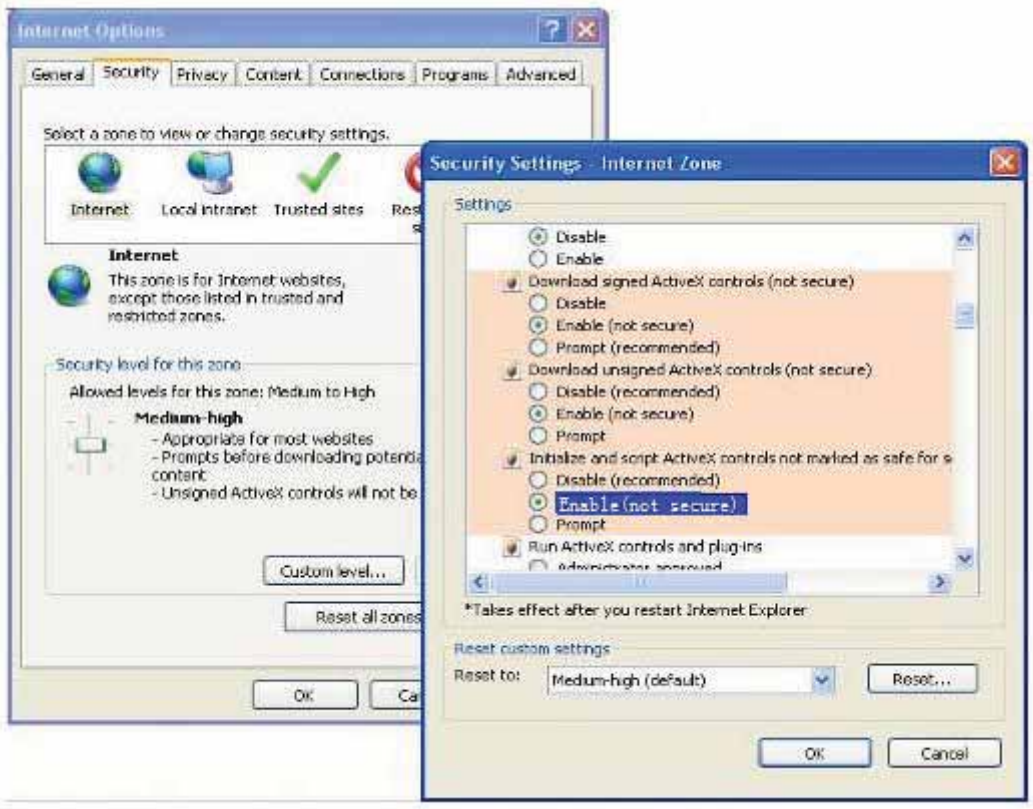


Figure 5.20

If you allow the ActiveX running, but still could not see living video. Please change another port number to try. Don’t use port 8000.

Figure 5.21

NOTE: Make sure that your firewall or anti-virus software does not block the camera or ActiveX. If you could not see video, please shut down firewall or anti-virus software to try again.

5.1.8 Can't access IP camera in internet

There are some reasons:

1、ActiveX controller is not installed correctly

2、The port which camera used is blocked by Firewall or Anti-virus software. Please change another port number and try again.

3、Port forwarding is not successful

Check these settings and make sure they are correct.

5.1.9 UPnP always failed

UPnP only contains port forwarding in our recent software. Sometimes, it may be failed to do port forwarding automatically because of firewall or anti-virus software. It also has much relation with router's security settings. So we recommend you do port forwarding manually. You can view your camera in internet successfully after you do port forwarding manually in your router(Figure 4.30).

5.1.10 Camera can not connect wireless

If your camera could not connect wireless after you set wireless settings and plug out the cable. Please check whether your settings are correct or not.

Normally, camera can't connect wireless mainly because of wrong settings.

Make sure broadcast your SSID; use the same encryption for router and camera.

5.1.11 Can't see other cameras listed in multi-device when using remote access

If you want to view all the cameras via the WAN, verify that each camera added in the multi-device settings can be accessed by using the DDNS name and port number. Use the DDNS domain name not the camera's LAN IP. (For more details see: How to add cameras in WAN)

5.2 Default Parameters

Default network Parameters

IP address: obtain dynamically
Subnet mask: obtain dynamically
Gateway: obtain dynamically
DDNS: Embedded FOSCAM domain name

Username and password
Default admin username: admin with a blank password

5.3 Specification

ITEMS		FI9851P
Image Sensor	Sensor	High Definition Color CMOS Sensor
	Display Resolution	1280 x 720 (1.0M Pixels)
	Min. Illumination	0 Lux (With IR Illuminator)
Lens	Lens Type	Glass Lens
	focal length	f:2.8mm，3.6mm/4mm/6mm/8mm Opention
	Aperture	F1.2
	Angle of View	70°
Video	Image Compression	H.264
	Image Frame Rate	30fps(60Hz), 25fps(50Hz), downward adjustable
	Resolution	720P(1280 x 720), VGA(640 x 480), QVGA(320 x 240)
	Stream	dual stream
	Image adjustment	The hue, brightness, contrast, saturation, sharpness are adjustable
	Flip image	flip and mirror
	Infrared mode	Automatic or manual
	Night visibility	With 13pcs IR-LEDs, Night Vision Range up to 10m
Network	Ethernet	One 10/100Mbps RJ45 port
	Wireless Standard	IEEE802.11b/g/n
	Data Rate	IEEE802.11b: 11Mbps(Max.); IEEE802.11g: 54Mbps(Max.); IEEE802.11n: 150Mbps(Max.).
	Wireless Security	P2P, WEP, WPA, WPA2
	Network Protocol	IP、TCP、UDP、HTTP、HTTPS、SMTP、FTP、DHCP、DDNS、UPnP、RTSP、ONVIF
System Requirements	Operating System	Microsoft Windows 2000/XP, Vista, 7,8; Mac OS
	Browser	Microsoft IE6 and above version or compatible browser; Mozilla Firefox; Google Chrome; Apple Safari.
Other Features	Motion Detection	Alarm via E-Mail, upload alarm snapshot to FTP

	Privacy Block	Set privacy area manually
	User Accounts	Three levels user role
	Firewall	Supports IP Filtering
	Reset	Reset button is available
Power	Power Supply	DC 12V/1.0A
	Power Consumption	4.2 Watts (Max.)
Physical	Dimension(LxWxH)	93(L)x 93W)x 82(H)
	Net Weight	290g
Environment	Operating Temperature	-20° ~ 55°C (-4°F ~ 131°F)
	Operating Humidity	10% ~ 80% non-condensing
	Storage Temperature	-20°C ~ 60° (-4°F ~ 140°F)
	Storage Humidity	0% ~ 90% non-condensing
Certification	CE, FCC, RoHS	
Warranty	Limited 2-year warranty	

Attention: Power adapter should be used between -20℃-40℃, and 20%-90% relative humidity.

5.4 CE & FCC

Electromagnetic Compatibility (EMC)

FCC Statement

Any Changes or modifications not expressly approved by the party responsible for compliance coulde void the user's authority to operate the 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.

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.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.This equipment generates,uses,and can radiate radio frequency energy and,if not installed and used in accordance with the instruction manual,may cause harmful interferece to radio communications.Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

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

5.5 Warranty

ShenZhen FOSCAM Intelligent Technology Limited.("FOSCAM") values your business and always attempts to provide you the very best of service.

No limited hardware warranty is provided by FOSCAM unless your FOSCAM product ("product") was purchased from an authorized distributor or authorized reseller. Distributors may sell products to resellers who then sell products to end users. No warranty service is provided unless the product is returned to an authorized return center in the region where the product was first shipped by FOSCAM or to the point-of-purchase, which may have regional specific warranty implications.

If you purchase your FOSCAM product from online store, please contact the point-of-purchase and ask for return/replacement/repair service.

Hardware Warranty Information

FOSCAM provide 2-year limited warranty for naked product and 6-month limited warranty for accessories.

Limited Hardware Warranty

FOSCAM products are warranted to be free from manufacturing defects in materials and workmanship starting from the shipping date of FOSCAM.

This limited hardware warranty does not cover:

- Software, including the software added to the products through our factory-integration system, software that included in the CD,etc.
- Usage that is not in accordance with product instructions.
- Failure to follow the product instructions.
- Abuse firmware upgrade without the authorized technician’s guidance.
- Normal wear and tear.

Return Procedures

- Please read FOSCAM warranty policy & policy of your reseller first before sending items back to point-of-purchase.
- Customer must first contact point-of-purchase to obtain a Return Merchandise Authorization (RMA) number before returning the product. If the product you received is suspected to be defective and the product warranty has not expired, The RMA number will allow your reseller to track your return much easier and help them expedite processing your request.
- After receiving your RMA case number, pack the item(s) very well with the original box and all the original accessories included such as power adapters, brackets, cables, manuals, and driver CD disks.
- Write your RMA number and the return reason (the problem of the product) on the warranty card along with the complete package to send them back.

Replacement Services

- **If customers ask for replacement service, please contact point-of-purchase and follow their policy.**
- Our technicians will inspect all items returned for replacement requests. If the retuned product is found in working order, we will return the same item received. However customers shall be responsible for all shipping & handling charges incurred for getting the units back to customers.
- If returned products are found defective, we will replace the product and assume the shipping cost for sending back the replacement unit to customers.
- If for any reason, we are unable to provide a replacement of the original returned item(s). You will have a choice for a “Substitute” item at the same equal value.
- We do not provide exchange and replacement due to normal hardware upgrade according the market after 14 days after the product is delivered.
- Our technicians will test the product before send out the replacement, any other demand for more than two times replacement for the same product during replacement limit will be rejected.
- **Replaced products are warranted from the balance of the former warranty period.**

Warranty Forfeiture

- Warranty is void if purchase from unauthorized distributor or reseller.
- **Warranty is void if trade-mark, serial tags, product stickers have been removed, altered or tampered with.**
- Warranty is void for mishandling, improper use, or defacing the product.
- **Abuse firmware upgrade without the authorized technician’s guidance.**
- Warranty is void for physical damage, altered, either internally or externally, improper or inadequate packaging when returned for RMA purposes.
- Warranty is void if damage has resulted from accident, dismantle, abuse, or service or modification by someone other than the appointed vendor, souse, fission or the spare part has been over the period of warranty.
- Warranty is void if product is damaged due to improper working environment or operation. (For example, improper temperature, humidity, unusual physical or electrical stress or interference, failure or fluctuation of electrical power, static electricity, using wrong power adapter, etc.)
- Warranty is void if damaged by the use of parts not manufactured or sold by FOSCAM.
- Damage caused by improper installation of third-party products.
- Warranty is void if damaged for irresistible cause, such as earthquake, fire, lightning, flood, etc.
- Product beyond limited warranty.

Shipping Fee

- If products are defective or damaged under normal use or operation in the replacement limit, distributors or resellers are responsible for the shipping cost the product back to customers, customers should assume the shipping cost send the product to the point-of-purchase.
- During replacement limit, if customers ask for replacement due to the product does not fit for customer’s personal expectation, customers should responsible for both shipping fee.
- Customers shall be responsible for both shipping fee if their product beyond the replacement limit but still in warranty limit.

Repair Service Out Of Warranty

- FOSCAM provide extra repair service for product that out of warranty, it is chargeable. The total fee contains device cost and service fee. Device cost (including accessories) is the standard uniform price provide by FOSCAM.
- Different region may have different service fee, please contact the point-of-purchase to confirm that before you ask for this service.
- Our technicians will quote the total price after detect the product, If customers refused to repair after the quotation, customers need pay for the test fee, $3.5/hour. If agree with the quotation, test will be free.
- Repaired product out of warranty will obtains 3-month warranty from the date of the product back to customers.

Limitation of Liability

- FOSCAM is not responsible for other extra warranty or commitment promised by resellers, if your reseller promised some extra commitment or warranty; please ask for written documents to protect your rights and interests.
- FOSCAM does not offer refunds under any circumstances. Please contact the point-of-purchase and follow their refund/return policy.
- FOSCAM shall not be liable under any circumstances for any consequential, incidental, special or exemplary damages arising out of or in any connection with this agreement or the products, including but not limited to lost profits, or any claim based on indemnity or contribution, or the failure of any limited or exclusive remedy to achieve its essential purpose or otherwise. Purchaser's exclusive remedy, as against FOSCAM, shall be the repair or replacement of defective parts. If FOSCAM lists a product on its website specification in error or that is no longer available for any reason, FOSCAM reserves the right to explain it without incurring any liability.

All rights reserved. FOSCAM and the FOSCAM logo are trademarks of ShenZhen FOSCAM Intelligent Technology Limited., registered in the U.S. and other countries.

6 Obtaining Technical Support

While we hope your experience with the IPCAM network camera is enjoyable and easy to use, you may experience some issues or have questions that this User's Guide has not answered.

If you have problem with FOSCAM IP camera, please first contact FOSCAM reseller for solving the problems. If our reseller cannot provide service, please contact our service department: **tech@foscam.com.**