SHARX SECURITY®

| **SHARX SECURITY INC.** | WIRED/WIRELESS IP NETWORK CAMERA USER GUIDE |

New mini HD outdoor model:
- Full HD 1920 x 1080 resolution
- Video with audio on PC, Mac, iPhone/iPad
- Wired/PoE or Wireless b/g/n networking
- MicroSD and NAS recording

V*IPcella*™ series cell phone enabled IP camera
Models SCNC3904, SCNC3904-WIDE

Introduction

Congratulations! You just purchased one of the finest IP network cameras currently available. All models have MicroSD memory card support, and for the 2015/2016 model year all our cameras support full high-definition video.

Shown here is an un-modified screenshot of the video quality of one of the most affordable Sharx Security outdoor cameras.

Using a Mac, PC, or iPhone/iPad you can view high quality live streaming video with audio direct from the camera. It is excellent for applications such as security & surveillance, as well as remote observation over the internet. Video recording is as easy as checking a checkbox in the task management menu.

The camera also supports mobile viewing of live video or snapshots using the latest version of Android. Other viewing devices may be added in the future.

Many common usage scenarios are handled directly by the camera's built in web server without the need for any software installations, downloads, accounts or monthly fees beyond your standard internet service.

Setup of the camera is mostly automatic if you have a current, industry standard router with the "Universal Plug and Play" feature (UPnP). Examples are NetGear R6100 or Asus RT-N56U. Older routers and some models provided by internet service providers may require a few manual setup steps to enable remote viewing. Recent versions of Apple Airport routers are fully supported by Sharx Security with our detailed, step by step setup instructions.

After you are familiar with the basic functionality of the camera you can enjoy many additional advanced features. For instance, you can enable the automatic sending of motion detection email alerts or automatic uploading of pictures to DropBox or other online servers using File Transfer Protocol (FTP).

An exciting new feature is the ability to turn the camera into a DVR (Digital Video Recorder) by recording video or pictures to the MicroSD memory card.

You can even turn the camera into a standalone NVR (Network Video Recorder) by enabling functionality to save video files to a network server.

This could be a commercial FTP server on the internet or your own standalone NAS (Network Attached Storage) hard drive. These features do not require a computer. Some customers prefer to use a computer for recording video, especially for recording multiple cameras, and that is supported with optional software such as the $59.95 BlueIris for PCs or the $30 EvoCam for Macs.

In our experience, we find that our customers get comfortable with advanced features quickly and then start using the camera on a daily basis to keep in touch with their home or loved ones.

This requires a reliable network connection. If you have an older router that is not up to the task, we highly recommend upgrading to one of the current models *before* you proceed with the camera setup.

It is important to note that you do *not* need an expensive router. Even current $40 - $80 units from NetGear, LinkSys, Dlink or Asus are perfectly fine. In fact, the most expensive routers that have too many nonstandard enhancements can often be less desirable than the reliable mainstream 802.11 b/g/n models.

With an up to date router you'll enjoy faster overall performance, better wireless transmission range, and improved network security. If you have the NVG589 router used by ATT/uVerse, please refer to the back cover page.

Super fast setup (for experts only)

If you are very familiar with IP cameras and would like to proceed as quickly as possible to see live and recorded video with wireless and remote operation:

1) Connect the included power supply to power and to the camera, and connect the included network cable to your router and the camera.

2) Find the camera's IP address in your router's attached device list (DHCP list) and then reserve the IP address so that it doesn't change, unless you have an Apple Airport, in which case you would use Airport Utility to reserve an IP address such as 10.0.1.2 based on the camera's MAC address (printed on the tag on the cable or sticker on the back)

3) Type http:// and your camera's IP address into a browser, click on "Enter" and log in with username: admin, password: admin, and if you are using Internet Explorer on a PC, allow both ActiveX installations

➔ **At this point you should already see nice video from the camera!**

4) Go to the task management menu, place a checkmark on task #9 and "Apply" to start motion detection recording, then briefly walk or wave your hand in front of the camera, then wait 2 minutes for recording of the first file to complete, and then check the "browse storage" menu

➔ **At this point you should have your first recorded video!**

5) For wireless cameras only: please attach the antenna. Then go to the camera's wireless setup menu, "search" to find your network and "apply", type and re-type your password and "apply" again to save it, then "test" to confirm that you have no typo, and disconnect the cable

➔ **At this point your camera should work wireless!**

6) Assuming you have a plain cable modem and a standard router with UPnP, click on "System" at the top of the settings screen and scroll down to see the internet URL. If it says "no UPnP gateway", enable "DMZ" or "default server" in your router for the camera's IP address, then get the internet URL from www.checkip.org . If your modem has a router also enable DMZ in the modem for your other router's IP.

➔ **At this point you should be able to access the camera remotely!**

For details and additional features, please refer to the following pages.

Contents

Pre-requisites and Setup Overview

This manual applies to the Sharx Security SCNC3904 and SCNC3904-WIDE. Besides the camera itself, and power for the camera, you only need:

- **PC or Mac with internet browser.** This is only required for initial setup only. Later the camera can work by itself without any computer present at the camera location.

- **A wired or wireless router with an available Cat5 wired network jack.** For wireless cameras, your router's wired network connection is only needed for initial setup. If no Cat5 jack is available, see Appendix A

- For standalone recording without a computer, the required class 10 **MicroSDHC memory card is already preinstalled** in all Sharx Security cameras. Any user supplied cards must be formatted in a specific way before first use in the camera, see page 41 and 55 for details

You can start using the camera on your own network immediately after powering the camera up and connecting the Cat5 cable to your router. You just need to look up the IP address that your router assigned to the camera and type it into a browser and log in with username: **admin** password: **admin**

However, depending on the capabilities of your router and the functions you intend to use, there are additional setup steps that are typically needed:

- **IP address reservation:** required on most routers to prevent the camera's IP address from changing whenever the router is restarted

- **Wifi setup :** required if you intend to use the camera wireless

- **Remote access setup:** required for access over the internet if you do not have a router that has already done this automatically with UPnP

- **No-IP hostname setup:** highly recommended if you have DSL internet

- **Email or DropBox setup:** required if you want motion detection alerts

- **Stream setup:** recommended if you have multiple cameras, intend to record to MicroSD or NAS, or intend to use multiple camera functions

- **Optional**: enable additional functions such as recording with or without motion detection, emails, uploads, or NAS drive storage

Initial Connection

All cameras come with a Cat5e network cable for initial connection of the camera to one of the LAN jacks of your router. Should you wish to set up wireless operation, this initial wired connection is required to tell the camera what your wireless network name and password is. You would also connect the small antenna now, making sure it is finger tight.

IMPORTANT: Make sure the Cat5 network cable is plugged into your router, not the computer, even if your computer has a network jack. If you don't have a router you'd need to get one, as this is one of the few prerequisites.

The camera also needs power. For the initial connection it is probably easiest to simply plug the included AC adapter into a wall outlet and then connect the power cable to the matching cable connector on the camera.

Later you can skip the AC adapter if you have a network switch with the PoE feature, such as the Netgear GS108PE.

Look for the small LED in the front of the camera to light up indicating that the camera has power. It should blink once or twice during the initial 45 seconds as the camera starts up. After about a minute, this LED also blinks whenever the camera is attempting to communicate over the network. Since viewing video involves sending a steady stream of data, this light will flash continuously when the camera is transmitting video. If this is not desirable, this light can be turned off easily in one of the camera's menus.

If you haven't already done so, please be sure to connect the Cat5 cable from the camera to one of the LAN jacks of your router. You should see the port light of your router light up to confirm a wired network connection.

To get started using your camera, you need to know the IP address that your router assigned to the camera. Then by adding http:// in front of this IP address you get a web link to the camera's built-in web server.

The following Quickstart sections will show you how to find the camera's IP address in your router, and how to reserve it so that it always stays the same.

Proceed to the **Mac Quickstart** section if you have a Mac with Apple Airport Extreme or Time Capsule. Proceed to **PC Quickstart** section if you have a PC running Windows 7 through 10, or proceed to **Generic Quickstart** for Mac computers without Airport or for Linux and other platforms.

Mac Quickstart

This Quickstart section applies to a common configuration for Mac users:

You have a current version Apple Airport (Extreme, Time Capsule, or Express), and your Airport is directly connected to a DSL or cable modem.

In this section you will be interacting mostly with **Airport Utility**. Please note that **Airport Utility** (and this Quickstart section) does not apply at all if you do not have an Apple Airport router. In that case, go to Generic Quickstart.

Start Airport Utility by clicking on its icon in your Mac's **Utilities** folder. Now select your Airport by clicking on its picture, and then log in with your Airport password. If you have trouble with these initial steps, Apple tech support can help. Since Sharx Security does not sell routers, we cannot help with the basics of setting up your wireless network or with router login or password issues.

Next, click on "**Edit**" and you should now see a screen with several tabs at the top, including "Base Station", "Internet", "Wireless", and "Network".

Click on "**Network**" and verify that the "**Router Mode**" is "**DHCP and NAT**".

If it isn't, don't change it. It would mean that this Airport is not your main router. If you have multiple Airports, you'd need to exit out of Airport Utility and start at the beginning, selecting another Airport that is your main router.

Note: If your main router is not an Apple Airport, it means your Airport is used only to add wireless functionality to a wired router supplied by your internet provider. In that case this entire chapter would not apply and you'd go to the "**Generic Quickstart**" section in this manual to set up your main router.

With your camera powered up and connected to one of the Airport's LAN jacks, it is ready to use as soon as you reserve its IP address as follows:

Still in the "**Network**" tab, click on the "**+**" button at the bottom of the "**DHCP Reservations**" box, then enter a name for the camera such as "SharxCam1". Make sure the "**Reserve Address by**" option is set to "**MAC Address**".

Now enter the MAC address of your Sharx camera, which you can find on a sticker on the back of indoor models or on a tag on the cable of outdoor models. Be careful about typos. There are numbers from 0-9 and letters in the range of A-F only. There is no letter O, just number 0 and letter D. Typical Sharx Security MAC addresses start with 7C but this is dependent on the specific model.

An IP address of 10.0.1.2 is typically pre-filled in Airport Utility. Unless that conflicts with another reserved IP address, you can keep it as is. Then click on "**Save**", then "**Update**", and wait for the Airport to restart.

After the Airport is finished restarting, you can use your camera immediately using the IP address you just reserved. Simply add **http://** in front of it and open it in Safari, such as http://10.0.1.2 and then you should see the Sharx Security login screen for your camera similar to the following:

To see video, click on "Enter". Until you change it, the default login is Username: **admin** Password: **admin**

Now the Sharx IP camera should always be on your network at the IP address that you reserved, regardless of whether you're using the camera with a wired network connection or wireless after completing the wireless setup.

Note: If you have trouble seeing video using Safari in Mac OSX Yosemite, go to "**Preferences**", then "**Advanced**", and uncheck "**Stop plugins to save power**". It may be necessary to restart Safari after this setting change.

Note: if you have one of the earliest (UFO shaped) Apple Airports you should consider replacing it with a current generation router. These oldest Apple Airports are now obsolete and are not supported by Apple or Sharx.

Next you will probably want to set up the wireless connection, unless you prefer to use the SCNC3904 camera with a wired network connection.

To prepare your Airport for easiest and most reliable wireless connection to a Sharx camera, check the following settings using the Airport Utility:

1. If you have enabled the Guest network feature of the Apple Airport, please remember not to use it for the camera or for any computer or smartphone that is supposed to be able to view the camera. The entire purpose of a guest network is to allow only straight access to the internet without allowing access to any of your own network devices. Therefore if the guest network is working properly, it should deny access to the camera.

2. Typically we recommend setting **"Wireless Security"** to **"WPA2 Personal"**. On the camera, this corresponds to Security Mode: **"WPA2-PSK"** with the Encryption Type: **"AES"**

   Very old Apple Airports (without the 802.11n option) need WPA security which is only available if you select the mixed mode **"WPA/WPA2 Personal"**, and in this case the camera needs to be set up with "**WPA-PSK**" with encryption type: "**TKIP**", not **"AES"**.

3. When using the recommended **WPA+TKIP** or **WPA2+AES** security, make sure your wireless password is between 8 and 63 characters and does not contain punctuation such as apostrophes ` ' " or brackets, or any non-English characters. For best compatibility with all wireless devices we recommend to use only upper case and lower case letters and numbers and no other characters. Please note that this key (password) is case sensitive. The older WEP wireless security is not recommended for using Sharx cameras with Apple Airport.

4. If you have set up your network with extra tight security using the "Access Control" feature in the Airport Utility, then you will need to add the camera's MAC address to the list of devices that are allowed to access the network. Be careful about typos.

5. If you have set up your wireless network as "Closed" with a hidden name, it is highly recommended to temporarily set your network into a normal configuration with a visible network name. Otherwise your camera will not be able to see your network as one of the available choices to connect to. After setup is complete, you can hide your network name again. In general, a hidden network name adds more confusion than actual security. There are tools that can reveal hidden names easily, so a hidden network is not an effective security method.

After you've checked the above settings, proceed to the section titled Wifi Wireless Setup.

PC Quickstart

This Quickstart section applies to the most common configuration for PC users: You have a current generation router such as NetGear, LinkSys, Dlink or Asus connected to a standard, non routing DSL or cable modem, or you have a combination modem and router which has all functions in one box.

Some of our customers have more complicated networks because they have added a wireless router to a wired router, or have business firewalls or VoIP boxes in front of the main router. In those situations we recommend that you consult an expert to simplify your network by eliminating redundant routers or placing all but one router into bridge mode.

With your camera powered up and connected to the router, some PCs will automatically discover the camera and show you an icon in the network device list. On Windows XP this list is called "**My Network Places**". On Windows 7 through 10 it is just called "**Network**". If you don't have a "**Network**" icon on your desktop already, you can get to it by clicking on the Windows "**Start**" menu at the bottom left, then click on "**Computer**" on the list at the right, and then click on "**Network**" in the list on the left, immediately below "**Computer**".

However, some PCs and routers do not have the **UPnP** Universal Plug-and-Play feature enabled. In following we will show alternate ways to find the local IP address that your router has assigned to the camera.

If you are familiar with your router's menus you can log in to your router and see the IP address for the Sharx SCNC series network camera in one of your router's LAN or "home network" status screens. By the way, in this document we're using the words "router" and "gateway" interchangeably.

For PC users, we also supply a program called **CameraSetup**. It is available for free download from www.sharxsecurity.com/downloads. If you install this program on your PC, it will tell you the addresses of all current and older Sharx cameras on your network. If this is the first time you are running the program you may need to click "Refresh" several times. You can use this program to set up cameras but we recommend that you use this program *only to find your IP address*. Then do all setup by going directly to the camera using the IP address, either by double-clicking on the address or by typing the IP address into your browser (some browsers need http:// in front)

If no camera is found it could be that your Antivirus or Firewall program is blocking the **CameraSetup** program. In that case you should either disable

your Firewall program or use the alternate method of finding the IP address by checking the menus in your router as described in the next section.
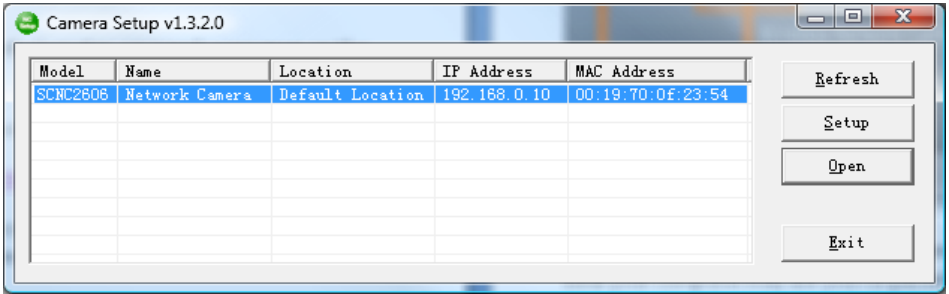
Regardless of the method you used to find your camera's IP address, once you've clicked on the icon or entered the IP address manually into your browser (with http://), you get to the main login screen for the camera:

To see video, click on "Enter", then username: **admin** and password: **admin**.

When using the camera for the first time on a PC with Internet Explorer, your PC will ask you for permission to install the viewing software (called ActiveX).

This ActiveX is needed to display the video stream and control the camera. Click to OK this at the top of your screen, then again click on OK on the install menu that will pop up in the middle or bottom of your screen. If you have a popup blocker like Norton or Google Toolbar you will need to disable it. Within a few seconds you can then see live video from the camera.

Internet Explorer also has a quick-record option that you can activate by adding your camera's IP address to the "Trusted Sites" list as follows: Go to the IE "**Internet Options**" menu, then the "**Security**" tab, then "**Trusted sites**", and with the checkbox for "**Require server verification**" unchecked, you'd click on "**Add**", then "**Close**" and "**OK**". Then the 3 icons shown above allow you to save snapshots, record video, or configure options.

To complete the camera setup, it is easier if you close all video windows and go to the main login screen again, then instead of clicking on **Enter** you would just click on **Setting**. Now proceed to the section titled Wifi Wireless Setup.

PC Only: Troubleshooting Internet Explorer Settings

On PCs, Sharx Security cameras are compatible with Internet Explorer 9 – 11 as well as Edge, Chrome, Firefox or Safari. The following troubleshooting info is **only for Internet Explorer**. For all other browsers, please refer to page 32.

If you find that your Internet Explorer window looks oddly shifted, please check the zoom level / magnification of your browser. It should be at 100% for proper viewing of the camera since Internet Explorer cannot zoom a live video stream. You get to the zoom menu through the gear icon at the top right:

Click on the gear icon, then select Zoom 100%
If you have 3 dots here, you are using Edge and not
Internet Explorer, so this section would not apply

If you used "refresh" and have a black video screen, close and restart the Internet Explorer window since it cannot refresh a live video stream.

If the camera has trouble installing the required ActiveX software, it could be due to one of the following reasons:

1) If you have nonstandard Internet Explorer settings, your should reset your Internet Explorer to defaults by going to the Tools menu or the gear shaped settings icon, then Internet Options -> Advanced -> Reset…

2) If this is a work environment where your IT department has set restrictive settings, ask them to temporarily lower the restrictions so that you can install the Sharx Security ActiveX. Installation is only required once.

3) If your computer has separate icons for the standard Internet Explorer and the 64 bit version, please be sure to use only the standard icon, not the 64 bit version. On Windows 8 and 8.1 please note that you must start Internet Explorer from the traditional desktop, not the tiled interface.

4) If you have old or overly aggressive Antivirus or Firewall software we recommend that you uninstall that software and use the free Microsoft Security Essentials instead. Similarly, be sure that you do not have any popup blocker software such as the ones bundled with Google, MSN, Bing or Yahoo toolbars. With a popup blocker it could be that you would miss the question about whether it's ok to install the Sharx ActiveX, and as a result it would not get installed and you wouldn't see video.

Generic Quickstart

The previous Quickstart sections showed you how to obtain the initial IP address of the camera if you have a Mac or PC with typical configuration.

In other cases it may be easiest to log into your router's web based setup menu. For the exact details you may need to refer to your router's manual, usually available for download on the router manufacturer's support web site.

Typically you access your router's web menu by typing the router's IP address into a browser window. Common router IP addresses are: http://192.168.0.1, http://192.168.1.1, http://192.168.10.1 , or http://192.168.1.254

Once you're logged into your router, you would look for a status screen or menu that mentions LAN or DHCP client list (LAN means local area network).

Typically there is a list of attached devices, and among these it is easy to pick out the IP camera since the name starts with SCNC, or there will be a 12 digit number that matches the number on the tag or sticker of the camera.

Regardless of the method you used to find your camera's IP address, once you've clicked on the icon or entered the IP address manually into your browser (with http://), you get to the main login screen for the camera:

To see video, click on "Enter", then username: **admin** and password: **admin**.

To complete the camera setup, it is easier if you close all video windows and go to the main login screen again, then instead of clicking on "Enter" you would just click on "Setting".

Reserving the Camera's IP Address

Some routers tend to remember and keep the camera's IP address as it was the first time you plugged it in.

However, many current generation routers tend to re-assign all IP addresses every time the router or a camera or computer is restarted. Aside from the inconvenience of having to find the camera's current IP address again, this can also interfere with some of the other setup steps.

Therefore it is important to check if your router has an address reservation menu, sometimes also called "DHCP reservation" or "Static DHCP".

On NetGear routers you click on the "LAN setup" menu on the left under the "Advanced" heading. **Linksys E series** routers tend to have a button for "DHCP reservation" in the middle of the basic setup screen.

Most routers show you a list of currently attached devices for which you can reserve the IP address. Typically you just select the device and then click on "Add" or "Reserve", which moves the item to the list of reserved addresses.

Then you typically click on "save settings" or "update" to make this choice permanent, and from now on the camera's IP address is locked and will not change even after power failures or restarts.

This allows you to add the camera's IP address to your browser's bookmarks or favorites menu and gives you a convenient way to login to the camera.

On current generation **Apple Airport** routers the address reservation menu is very different. Please refer to the MAC Quickstart section for details.

On older Apple Airport routers, older Linksys routers such as WRT-54G, and some of the freebie routers provided by the DSL internet companies such as ATT and Verizon, there is unfortunately no address reservation menu.

In that case, the IP address needs to be set up in the camera as shown in the chapter titled "Manual Setup Step 1: Assigning a Permanent IP Address for your Camera".

To summarize: **If you can find your router's address reservation menu, you should use it now to lock the camera's IP address in the router. If you cannot find your router's address reservation menu, you would set up the camera's IP address manually, <u>but do not try both methods at the same time.</u>**

Wifi Wireless Setup

Most likely your wireless network was set up with a password (also known as wireless key). If you don't remember it, you can check your router's wireless setup menu or ask the person who set up your wireless network.

Without your password you *cannot* proceed with your camera's wireless setup, so you can either continue to use your camera in wired mode or set up a new password in your router. Another possibility is to disable passwords in your router but an unsecured wireless network is not recommended.

Clicking on "Setting" from the main camera login screen will get you to this:
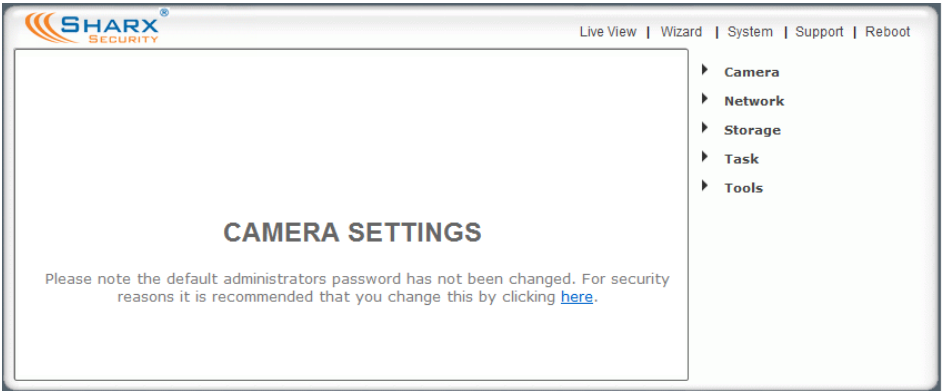
Click on "Network", then click on "Wireless", and you'll get to this screen:
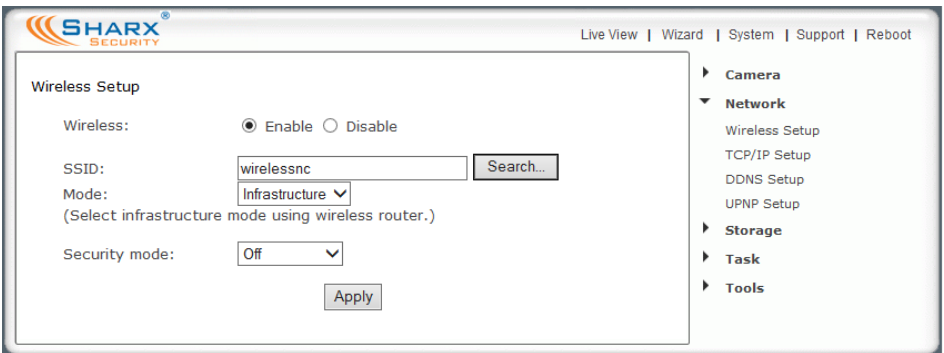
Do NOT type anything in the SSID field. Instead, use the "Search…" function so that your camera can tell you which networks it can see:

SSID List

	SSID	Mode	Channel	Auth	Encrypt	Signal
◉	SharxOffice	Infrastructure	1	WPA2PSK	AES	.ıll
○	DSSIWIFI	Infrastructure	2	WPA2PSK	AES	.ıll
○	Apple Network e108cb	Infrastructure	6	WPA2PSK	TKIP/AES	.ıll

OK Cancel

You may see a whole list of networks in your neighborhood. Select your network among this list, then click "Apply", and check if your network name has now been filled into the SSID field. If nothing shows up, try "Search" again, or un-hide your network name if your router is configured as a closed system. Also please double check if you connected the antenna to the camera.

Be sure to close any live video windows while trying to configure the wireless feature. If you've skipped ahead to recording, you may want to disable it now.

Please make sure "Infrastructure" is selected before proceeding, since that is the most common type of network. "AdHoc" is for network experts only.

The "Security mode" needs to match the type of wireless password used on your router exactly. The old type is WEP. Newer routers may use WPA or WPA2 passwords (keys).

Not sure what you have? Check your router's wireless setup menu. In general it would be a good idea to use WPA2 in your router, and more specifically the combination of WPA2 with AES. However, if you are comfortable with your existing wireless security and do not feel like changing, you can also use the older WPA or the very old WEP wireless security. First we will show the setup for WPA2 or WPA and then we show the setup for the older WEP security.

Current Apple Airport and most new generation routers use WPA2 with AES:

However, older Apple Airport and many other routers use WPA with TKIP:

Please remember that both WPA and WPA2 keys are case sensitive and need to be between 8 and 63 characters. Please note: do not use the quote or apostrophe characters ` " ' or any non-English characters.

When you have entered the key, click on "**Apply**". You'll get a message about "wireless setup accepted successfully" but that only means that the password was stored in the camera. You're not done yet until you use the "**Test**" button to check if you typed it correctly. (Be sure to click on "**Apply"** before "**Test**")

If the test reports "**Wireless connected**" you can remove the network cable and it should work wireless after a short delay. If the test reports "**No wireless connection!**"please double check your key (password) and refer both to the Wifi troubleshooting and "Known issues" section of this User Guide.

If you have WEP passwords, the procedure is similar:

In almost all cases you would select Authentication to be "Auto"

The next setting is critical, so you need to be careful to select the right choice. Some laptop computers are more forgiving and will connect anyway, but the camera needs to know **exactly** what type of WEP encryption is used. Fortunately there is a way to tell based on the exact number of characters used in your encryption key.

- Key length 5 characters = **WEP64** with **ASCII**
- Key length 13 characters = **WEP128** with **ASCII**
- Key length 10 characters = **WEP64** with **HEX**
- Key length 26 characters = **WEP128** with **HEX**

For example, Verizon often sets up their DSL modem / Wifi router with a password similar to the customer's telephone number, which is 10 digits and therefore implies WEP64 and HEX. Some routers are configured for a key index other than the factory default of 1. This is very rare.

When you're done, click "**Apply**", then "**Test**".

Important: Do not forget to click on "Apply" before you leave the page. Without "Apply" the wireless settings that you tested will _not_ be saved.

If the test reports "**Wireless connected**" you can remove the network cable and it should work wireless after a short delay of about 30 seconds.

Congratulations! At this point you should be able to use your camera wired or wireless on your local network using the same local IP address.

If it doesn't connect, we recommend that you temporarily remove wireless security from your router for a quick experiment to see if the setup succeeds with no passwords. Then put the password back in and try again. Many times this will refresh your memory about the exact spelling of your password.

Also, it could be either that the camera is too close to or too far from your router, or that your router was set up with the tightest possible security which allows only known devices to connect to your network. In this case, you'd add the MAC address of this camera to your allowed list. In this context, MAC refers to a hardware network address and is unrelated to Macintosh. The camera MAC address is printed on a tag on the SCNC3904 cable.

During setup it is best to have the camera at least a couple of feet away from the antenna of the wireless router. The maximum distance is dependent on the kinds of walls and objects that are between your wireless router antenna and your camera. A distance of 75 ft across and 1 floor up/down is typical.

One easy test for determining the maximum recommended distance is by using a laptop at the intended camera location. If your laptop shows at least 50% signal strength at that exact same location then the camera should be ok too. Any less than that may be unreliable, so you may want to move your router or the camera, or adjust the angle of your router's antennas.

Keep in mind that the wireless signal travels easily through common building materials such as wood, glass, sheet rock, and vinyl siding, but does not go at all through metal. Concrete with metal rebar can be a real challenge.

If there are any big metal objects such as a fridge, filing cabinet, or HVAC ducting in between the Wifi router and the camera, try to reposition either the camera or the router so that the metal object doesn't block the signal.

Also, many microwave ovens and older 2.4 GHz cordless phones may interfere with all Wifi networking while in operation. Using a laptop you may not notice a pause, but with a camera that transmits or records video continuously any interruption will be much more obvious. Nearby Bluetooth devices such as cell phone headsets, Playstation game controllers, or a wireless keyboard and mouse can also interfere with wireless networks if the devices are too close.

The best placement for a wireless router is in an area that is higher up and free of nearby clutter, for example on top of a wooden book shelf.

Wifi Troubleshooting

If the camera does not connect and you've already checked the settings mentioned on the previous page and you made sure the antenna is connected properly, please log in to your router and double-check the setting for wireless channel selection. On an Apple Airport you would use the Airport Utility.

On N mode routers other than current Apple routers be sure to turn off "**wide channel spacing**", sometimes also referred to as "**40 Mhz mode**" or "**up to 300 mb speed**". This is not compatible. You should use "**standard channel spacing**", also known as "**20 Mhz**" or "**up to 130 mb speed**". Mixed 20/40 Mhz should be avoided. (Apple routers no longer allow the wrong setting)

If the "search" function of the wireless setup page found your Wifi network it means that the wireless networking hardware is working. If it then doesn't connect it means that there is a password or IP address related issue.

You can temporarily turn off passwords on your Wifi router, and if you then set "Security mode" to "off" in the camera, it should connect unless you have set your router to reject connection attempts from unknown devices.

Assuming that you are now at least connecting without passwords, you can proceed to add wireless security to your router and try again. We recommend WPA2 if available, otherwise WPA. The older WEP mode is obsolete and may not work correctly on Apple Airport. If you have trouble, switch to WPA2.

Since each password type can have 2 variations, this means you could have 4 possible combinations: WPA-TKIP, WPA-AES, WPA2-TKIP, and WPA2-AES. Only WPA with TKIP and WPA2 with AES are valid, the others will not work reliably.

Some routers like Apple Airport series do not show clearly which one of these settings is being used, so if you have difficulty you should try both WPA + TKIP and WPA2 + AES. On a laptop you typically do not need to specify the exact password type since the laptop will try all everything automatically. The camera is more picky, it needs to know exactly what type of password you are using. It does not try anything other than the exact type that you entered.

Remember to "**Apply**" first, then "**Test**". If it says "**Connected!**" at the end of the test, you can remove the cable. Please note that as long as the cable is still attached, the camera's "**System**" menu will show "**No wireless connection**" since you are still using the wired network and only one network can be active.

If you still have trouble, be sure to check the Appendix for known issues.

Apple Airport Remote Access Setup

If you have a router other than Apple Airport, skip ahead to the next section.

In order to access the camera remotely from outside your network, you have to tell your Airport to allow access to the network ports used by the camera.

Go back to the "**Network**" tab in Airport Utility 6 as described on page 7. Notice there is a "**Port Settings**" box below the "**DHCP Reservations**" box you used earlier.

Click on the **+ (add)** icon below the "**Port Settings**" box. "Firewall Entry Type: IPv4 Port Mapping" should remain selected. Now fill out the box as shown:

Description:	**SharxCam1**
Public UDP port:	**30000-30001**
Public TCP port:	**8150**
IP address:	(add the IP address for your camera, e.g. 10.0.1.2)
Private UDP port:	**30000-30001**
Private TCP port:	**80**

Double check that you used the exact same IP address you reserved for your camera earlier, then click on "**Save**". For additional cameras add another entry for each IP address you reserved. All cameras use Private TCP port 80, but the next camera would have UDP ports 30002-30003, public TCP port 8151, and for cameras beyond that add 2 to the UDP ports and 1 to the public TCP port.

Then click on "**Update**". After your Airport is restarted, go to the "**Internet**" tab and write down the number you see in the field labeled "**IPv4 Address**". That's your external IP address. Someone from outside your network should be able to access your camera using this address with **:8150** added to the end. For example, if the IPv4 address is something like 12.34.56.78, you would enter the following in your browser: http://12.34.56.78:8150

Note: This assumes your Airport is your only router. You can check this by going to www.checkip.org with Safari. The IP address shown there should be exactly the same as the IPv4 address in your Airport. If not, you have multiple routers and networks. In that case, each preceding router would need to have a DMZ or "Static NAT" entry to forward all ports to the next router.

After completing this section, your Airport is set up to allow remote access to your camera. If you have DSL, proceed to "Choosing a name for your camera".

Is the Remote Access Setup already done?

If you have any current generation industry standard router other than Apple Airport, such as NetGear, LinkSys, Dlink, or Asus, it is likely that the UPnP "Universal Plug 'n Play" feature of your router has already done the setup for remote access. Your camera would already be visible from the internet to anyone who knows the IP address, usernames and passwords that you choose.

Keep in mind that there is a distinction between local (intranet) IP addresses, meaning IP addresses on your own network, and external (internet) IP addresses, which are unique in the entire world. With the UPnP feature enabled in your router, the camera's "System" menu can show you both:

1) the link (URL) for accessing the camera from your own network, often something like http://192.168.0.100

2) the automatically configured link (URL) for access from a remote location, often something like http://12.34.56.78:8150

A quick comment about ports: In general, IP addresses can have many different ports associated with them. When browsing to ordinary web sites there is usually no need to specify a port and that's why you may have never heard about ports at all. However, when different devices share a single IP address they are distinguished with a port. Basically a port has a similar function for an IP address as an extension on a telephone number.

Ports are specified by including the port number in the web address with a colon and the number after the .com or .net domain name. In the example shown above the port number is 8150.

If UPnP was available on your network, the camera has already set up the correct ports for remote access. A quick way to see the complete external IP address (URL) is to go to the **System** menu at the top of the **Setting** screen. Scrolling down to the UPnP section you will see the Internet URL (IP address).

Then all you need to do is to type either your internal (Intranet) or external (Internet) IP address in your browser, depending whether you're accessing the camera locally or over the internet. If UPnP worked, you can skip the manual IP address setup and proceed to selecting a name for your camera.

Note: if the system menu shows you an Internet URL (external IP address) that starts with 192.168 or 10.0, your DSL or Cable modem has a built in router. In this case, contact us with the model number of your modem for assistance.

Enabling UPnP for Automatic Remote Access Setup

If UPnP did not work, and if you have an up to date router other than Apple Airport, it is worth double checking if UPnP is enabled in your router. Some routers like the ActionTec and Westell units distributed for free with Verizon and Qwest DSL service have the feature initially disabled.

Usually it is very simple to enable UPnP. You just need to log in to your router's setup screen and find the UPnP menu. Then you click on enable, save the setting and restart both the router and the camera (in that order).

Many routers (e.g. LinkSys, Dlink) may need a firmware update for UPnP to be available or work properly. You should look up your router's model number on your router manufacturer's support web page to see if updates are available.

The camera comes from the factory with UPnP enabled. You can double check by selecting the "UPnP Setup" tab under the camera's "Network" menu:

If UPnP works, clicking on the camera's "System" menu at the top of the settings screen will show something like the following in the UPnP section:

UPNP port forwarding	
Status:	Success
Gateway external IP address:	67.189.236.71
Gateway external port:	8150
Internet URL:	http://67.189.236.71:8150

While it won't from your own network, you can test external access to your camera by emailing the Internet URL to someone at a different location.

Overview of Manual IP Address Setup (without UPnP)

In the previous section we showed how to tell if your camera was able to automatically configure itself using your router's UPnP feature.

In this section we provide an overview of the manual IP address setup procedure. You would only need to do this if UPnP is not available on your network, for example if you have an older router. If UPnP worked or if you have an Apple router that you've already set up with our Airport specific instructions please skip ahead to "Step 3: Choosing a name for your camera".

Most routers come pre-configured to protect your own network devices from external access. This means that in order to view your camera remotely over the internet your router needs to be configured to open ports and allow access. If this sounds difficult, you may want to consider upgrading your router to a newer NetGear, LinkSys, DLink or Asus model as they are very inexpensive now, even starting at $29.95

The terminology for opening up ports can be different based on the manufacturer of the router. Typically this setting is called "Web access", "DMZ", "Virtual Server", "Virtual Service", "Pin hole", "User Defined Service", "Port Forwarding" or "Port Mapping". There are 2 main steps involved in port forwarding:

1. Reserving a DHCP address or assigning a permanent (static) IP address for your camera on your local network.

2. Configuring your router to allow access from the internet to the camera's IP address on your local network.

Strictly speaking, step 1 above is optional, but some routers (especially LinkSys and Belkin models) tend to reassign all the IP addresses on your home network after a power failure or based on the order in which you use them. Therefore your setup is only reliable if you reserve a DHCP address or assign a permanent IP address to your camera and then do the actual port forwarding. Reserving an IP address in the router is easier than setting it up in the camera, so please check the section on reserving an IP address to see if your router supports it.

Some residential internet service providers want to charge more for business service and therefore deliberately block all internet access that looks like it might involve a web server at the standard port 80. That's why we always recommend using port 8150, which in our experience is usually available.

Manual Setup Step 1: Assigning a Permanent Local IP Address

Manually assigning an IP address for your camera is **only** necessary if your router **does not** have the address reservation feature. As discussed earlier in this manual, all current NetGear, LinkSys, Dlink and similar standard routers have an easy address reservation menu. The Mac Quickstart section shows how to use address reservation on a current generation Apple Airport.

If you have already reserved your camera's IP address you would skip the manual assignment of an IP address, so please skip ahead to the next section.

Old Apple Airport and old LinkSys routers, as well as many DSL modem routers do not have the address reservation feature so in that case the manual IP address setup as explained in this section is the only choice.

On your home network (LAN) all your computers and other network devices have a local IP address. In every IP address there are 4 groups of digits that can have a value of up to 255.

To pick a permanent address for your camera you first need to know your router's IP address. It is shown in your camera's system menu (at the top of the settings screen) if you scroll down to "Default Gateway". The router's IP address determines the first 3 groups of digits for your camera's IP address.

Now we need to select a valid number for the 4th group of digits. We don't simply pick a random number because we have to avoid numbers that are already taken or that could be assigned by your router.

The router uses addresses in a range set aside for this purpose (called the DHCP range). For many routers, this DHCP range is from 2 to 100 but you'll have to check your specific router's DHCP menu. Sometimes this is shown as start and end address, or start address plus number of available addresses.

Why is this important? We need to select an address outside this range to make sure that your router would never pick this address for another device.

For example, LinkSys routers use a DHCP range from 192.168.1.100 to 149, so you could choose 192.168.1.200 for the camera. Never use addresses that end in .0 or .1, since that is reserved for your router, and never use addresses that end in a number higher than 254.

There is one special case: some routers such as Comcast SMC business gateways have been preconfigured for a DHCP range of .2 - .255 which leaves no available IP address outside the range. In that case you first have to reduce the range by setting it to .2 - .199. Then you have addresses from .200 - .255 available for IP cameras, printers, and other devices needing a fixed IP.

Once you know your router's IP and have chosen a valid IP for your camera, go to the Camera Settings menu, then select "Network" and "TCP / IP Setup":

Click on "use the following IP address". Then enter the IP address you picked that is outside your router's DHCP range. Do not change the subnet mask. The default setting of 255.255.255.0 is correct unless you have a very unusual home network.

> Then enter your own router's address in the "Default Gateway" box and also in "Primary DNS IP address".

   IMPORTANT: Do not leave the "Default gateway" or "Primary DNS" fields blank. Your own router's IP address must be entered in both.

Note that the first 3 groups of digits of your default gateway should be the same as your camera's IP. Usually the last digit is 1, sometimes it is 254.

It is very important to add both the "Default Gateway" and at least the "Primary DNS" address when assigning a static local IP. While the camera gets this information automatically from the router when using DHCP, the camera will not obtain this information if a local IP address is assigned manually.

For primary/secondary DNS IP address it is also possible to copy the exact same IP addresses that are shown for primary/secondary DNS IP in your router's WAN or status menu, or Google's public DNS such as 8.8.8.8

SHARX ® SECURITY

Live View | Wizard | System | Support | Reboot

TCP/IP Setup

▸ Camera
▾ Network
    Wireless Setup
    TCP/IP Setup
    DDNS Setup
    UPNP Setup
▸ Storage
▸ Task
▸ Tools

○ Obtain an IP address automatically(DHCP)
◉ Use the following IP address
    IP address: `192.168..1.201`
    Subnet mask: `255.255.255.0`
    Default gateway: `192.168.1.1`

○ Obtain DNS Server address automatically
◉ Use the following DNS server address
    Primary DNS IP address: `192.168.1.1`
    Secondary DNS IP address: `8.8.8.8`

HTTP/RTSP port: `80`
RTP port range: `30000` -- `30200`

[Apply]

The HTTP port is usually 80. The RTP port range should start at 30000 for your first camera. For all additional cameras the start of the range increases by 2, for example your 2nd camera would have a starting RTP port of 30002, the 3rd camera would have 30004, 4th camera at 30006 etc. The RTP port range ending address should always stay at 30200.

At this point it's a good idea to double check your settings, and preferable take a screenshot or take notes. After you click on "Apply", you need to log in to the camera at the address you just picked. Remember to add the http:// in front of the IP address, as in http://192.168.0.101. If your port is not 80 you need to add a colon : and the port number at the end of the IP address, too.

If there is no response from the camera at the new IP address, please refer to the notes or screenshot you took before you applied the new settings.

If you catch a typo after you applied it, it is possible to recover from this in 2 ways. You can reset the camera back to factory default settings as described towards the end of this manual. Or you can temporarily set up your router such that the wrong IP address would work with it.

If your IP address assignment was successful, from now on, regardless of what computers or other devices you have on your own network and regardless of the order that you turn them on or off, your camera's IP address will always be the same. However, you have to make sure that you never give the same IP address to more than one device.

Manual Setup Step 2: Configuring your Router to allow Remote Access

If your camera was automatically set up with UPnP you would skip this section and proceed directly to Step 3: Choosing a name for your camera.

If you have only 1 camera, it is simplest to configure your router to use "DMZ" or "Default Server" for the camera. This basically means that any request from the internet is forwarded to your single camera. Many of our customers use more than one camera so we will explain the port forwarding procedure.

Special note about the NVG589 router commonly supplied by ATT/UVERSE: In our experience that specific router's port forwarding feature is hopelessly broken, so the only choices are to enable "Default Server" which works for one camera, or to add another router. Please contact us for details.

Port forwarding is sometimes called "virtual server", "user defined service", or "port mapping" and is explained in your router's manual or online help. The manual is usually available from the manufacturer's tech support web site.

Typically you need to provide a "service name" for each group of ports that is forwarded. The name could be anything that isn't already used, for example "Cam1HTTP" and "Cam1RTP". Then you typically need to enter the external (public) and internal (host) ports and select either TCP or UDP. For browser access to the camera you need to forward public TCP port 8150 to internal port (base port) 80. If you have an older LinkSys it may not have a distinction between public and private port. Then you'd have to change your camera's HTTP port to 8150 in the TCP/IP menu (shown on previous page), and then use that port even for local access (for example http://192.168.0.101:8150)

For cell phone access (RTP) you also need to forward UDP ports 30000 and 30001, however this time the external and internal ports are both the same. Your 2nd camera would use TCP port 8151 and UDP ports 30002-30003, the 3rd camera would use TCP port 8152 and UDP ports 30004 – 30005 etc.

After these settings, your router typically needs to be restarted and then you're ready to use the camera over the internet. First you need your router's IP address on the internet (that's NOT the local address that starts with 192.168). You can find this address by looking at your router's WAN menu, or you can use www.checkip.org

A friend who is outside your local network should then be able to access your camera using this IP address and port 8150, as in http://123.45.67.89:8150

Setup Step 3: Choosing a Name for your Camera on the Internet

So now you should have been able to have a friend see you on your camera. With typical residential internet service your router's IP address can change from time to time. Looking up the current IP address can be inconvenient, and buying a static IP address is an unnecessary monthly expense.

www.no-ip.com is one of the recommended companies for "Dynamic DNS" service. Also known as DDNS, this is a service that allows your own name to be used as a substitute for the camera's external IP address. Together with software in your camera this also makes sure the name for your camera is always updated with the correct IP address.

These DDNS companies are legitimate. They don't spam you and there's no catch, other than the requirement that you log in at least once a month to keep your free account active. They also have inexpensive paid annual service.

First you sign up to create a free account. We'll use www.no-ip.com as an example. The "Sign up" button leads to a "Create your No-IP account" form. The free account is sufficient. There is now a shortcut on the account creation form to sign up immediately for one hostname, but that shortcut doesn't appear to work for free accounts.

Once you have an account and once you validated it by responding to their email, log in and select "Hosts/Redirects" on the top left of the screen, then "Add Host". For Hostname, pick anything you like as a name for your camera, except do not use spaces or punctuation. Use only lower case letters and numbers. Then click on the down arrow for the second part of the name. There is a whole selection of free domain names you can pick from, as well as some that they consider premium names worth paying for. For example, you could pick **servehttp.com** as we have done for our demo cameras.

Then be sure that only "**DNS Host (A)**" is selected. Don't worry about the current IP address and don't change anything else. Click on "Create Host" at the very bottom and you're done! Please write down your complete hostname as well as the username and password you used for logging in to No-IP.com as you'll need it for the next step.

DynDNS.com is very similar but is no longer free, so we recommend No-IP.com

Now proceed to the next section to make sure your name is updated correctly. Note: **Do not download the update client or any other software from No-IP**

Setup Step 4: Automatic Updating of your Camera's Internet IP Address

In the previous step we set up a name for your camera. To make sure that this hostname always corresponds to the correct IP address for your camera we have to make sure it is updated automatically when there is a change.

There is no need for client software. Sharx IP cameras have a DDNS menu that allows you to enter your hostname information. This DDNS menu is under "Network" in the camera's "Settings". Be sure to select the correct DDNS provider, for instance if you signed up with No-IP.com you should select No-IP in the camera's DDNS menu.

After you enter your account and hostname information you can go to the camera's "System" menu at the top of the Settings screen and scroll down to the DDNS section to see if it worked. If it says "Updating" or "Unavailable" you should double check your account settings. No-IP.com uses your complete email address as username, and the password required in this menu is the one you created during No-IP account setup. If successful the camera will show you the complete external URL for your reference. Note: Only 1 single camera per network needs the DDNS setup. This enables access to the entire network.

Important Notes

1) If you try to access your own camera(s) from your home using the external IP address it may not work. Some internet service providers recognize that you are trying to do something that usually doesn't make sense. Their routers may block requests that go from your network out to the internet and then loop back to your own network.

   Therefore we always recommend that you get in touch with a friend to help you test the remote access to your camera from outside your own network. Or you can use an iPhone in 3G mode (Wifi turned off)

2) Once your camera is live on the internet, you should change the admin password to something only you would know. See the "User Management" menu under "Tools" section of your camera's "Settings" screen. Only **admin** can change settings. If you add other user names they can only see video without changing anything.

If you forget your password you can always reset your camera to factory settings using the reset procedure shown at the end of this manual.

Night Vision Settings

The SCNC3904 and other models with infrared (IR) night vision have several settings to adjust your preferred night vision.

The IR LEDs can be set to "On" or "Off". In addition, the "Automatic" setting uses a light sensor on the front of the camera to check ambient light levels to turn on the IR LEDs only at night.

Similarly, "Black & White Mode" can be "On", "Off", or "Auto". The default setting is "Auto" so that you have the highest sensitivity at night. Sometimes you have better picture quality with Black&White Mode "Off". It's worth a try.

The "Moonlight mode" setting tries to boost available light by reducing the frame rate. As with the IR LEDs there are settings for "On", "Off", or "Auto".

If you are using IR cameras to look through a window, you should set IR LEDs to "Off". Otherwise the IR LEDs would reflect off the window glass and the glare would make everything almost invisible. Moonlight mode on "Auto" should help if there is at least some available light.

All our current camera models have a feature that allows beautiful daytime colors as well as night vision in total darkness. During the day, an optical "IR cut filter" removes all infrared light to make colors look vivid and natural. At night, the filter moves out of the optical path to enable IR night vision. You can actually hear a click when this filter moves. This happens both during power-up and when light levels change between day and night. The click is normal.

If you are using the SCNC3904 to look through a window, you may want to experiment with the IR filter in the automatic position even though IR LEDs are set off. Combined with automatic moonlight and automatic black & white mode this makes the best use of available street lighting.

For special applications there is also a setting that allows you to keep the IR filter fixed either in the "on" or "off" position. The normal factory default is automatic and this is recommended.

IMPORTANT: For best IR night vision on outdoor cameras please refer to page 33 about the sunshade position. Clean lens cover glass also helps extend the range and reduces fogginess.

Video with Audio using Safari and Firefox Browser

When using a Mac to view the camera, or when using a PC with any browser other than Internet Explorer, the camera tries to figure out the best way to display the video. In some cases it will try to launch a plug-in such as Flash Player or Quicktime Player to display video with audio.

Current browsers have the required plug-ins already built in. On older PCs, if you don't want to use Internet Explorer, you might need to install **Flash Player** from Adobe.com or **Quicktime Player for Windows** from Apple.com

On browsers that support it, our cameras show links for "Primary Stream" or "Secondary stream" at the top of the window. The secondary stream has a smaller window and uses a lot less data. You can switch between the streams at any time. It will just take a few seconds to restart the new stream.
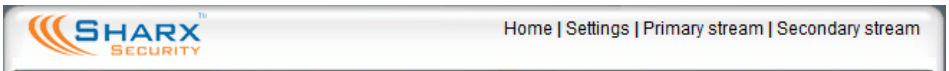
Please note that it is normal for Quicktime or Flash to show video with a few seconds of delay. Quicktime and Flash do this automatically to smooth over any network disturbances without causing interruptions in the live stream.

If you don't get audio, try the secondary stream, and double check that you did not inadvertently turn down the volume level for your computer. Also check the tiny popup Quicktime volume control shown in the pictures below:

  PC Quicktime   Mac Quicktime

bottom left   bottom right

A few interesting things to note: The Mac version of Quicktime has a double arrow icon at the bottom right, next to the volume icon. Clicking the double arrows expands your screen to full size. This comes in handy when watching one of our high definition cameras. There is also a pause/play icon at the bottom left of the window that is useful. However, the negative "time remaining" countdown at the bottom right of Mac Quicktime can be safely ignored as it doesn't really have any meaning for live streaming video.

On PCs some versions of browser plugins might not support full size viewing. In that case you could use Internet Explorer, where the square icon at the bottom right has the same function of expanding your window to full screen.

Mounting and powering the camera outdoors

Before mounting, you should first become familiar with the camera indoors.
Once installed outdoors, cameras cannot be returned for refund.

All our cameras have the industry standard mounting hole with ¼"–20 thread.
This is compatible with a wide variety of security camera mounts or tripods. If
you want to use a mount other than the one we supply, please be careful that
the new mount does not push the white reset button near the camera
mounting hole at the bottom of the SCNC3904.
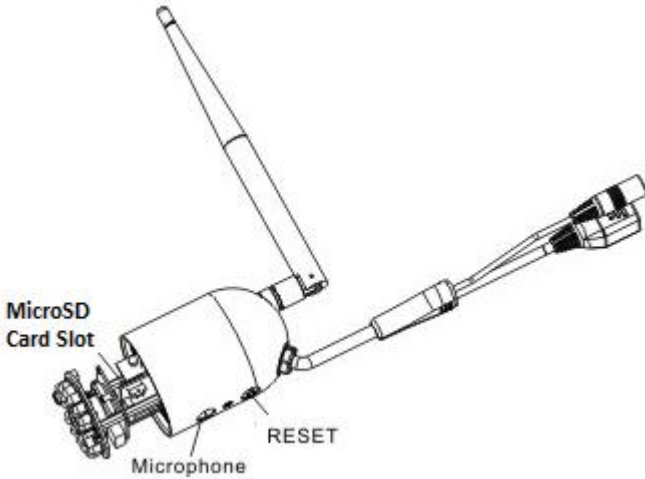
In a typical scenario the camera is mounted to a wall with the supplied
adjustable mounting bracket.
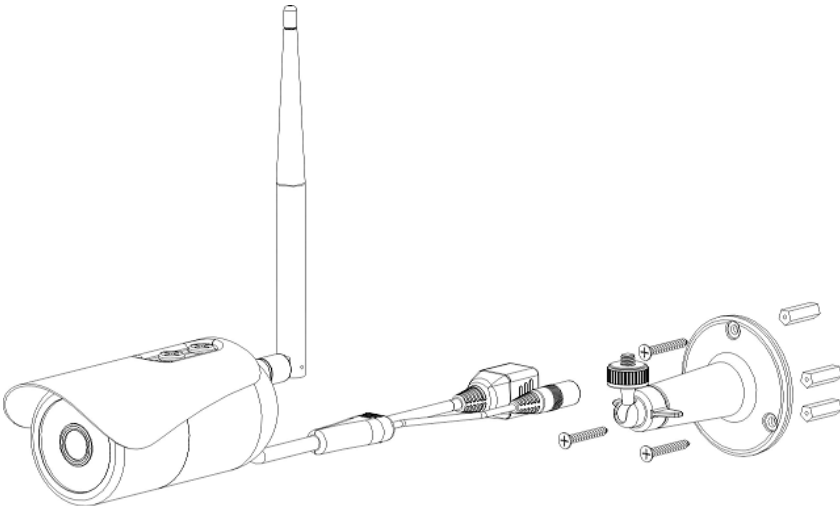
The easiest way to mount the outdoor camera to the wall is to mount the bracket all by itself to the wall first, using the 3 included screws or similar.

Then if you have the threaded mounting post facing forward and the wing nut slightly tightened, the camera can be rotated onto the mounting post without the cables getting in the way. Then you'd loosen the wing nut and position the slot in the ball joint upwards so that the camera can be directed to the desired viewing angle, and the wing nut and the white plastic disk can then be tightened to lock this position into place.

Alternatively you can replace one of the camera's sunshield mounting screws with the special silver colored hex mounting nut that is supplied in the hardware bag. This allows attachment of the mounting bracket from above if you are planning to install the camera under an eave or to a ceiling.

Note: Do not try to remove the silver colored disks at the bottom of the camera. One is the microphone and the other is the reset button. Attempts to remove those could cause damage to the camera.

Please note that the sunshade can be mounted in several positions depending on your needs. If it extends forward it can do a better job reducing glare from the sun as well as keeping the lens glass dry in light rain or snow. On the other hand, **reflections of IR light from the underside of the sunshade would make the entire picture appear foggy, so for maximum night vision range you should either move the sun shade all the way back or remove it entirely.**

A MicroSD card is already pre-installed in the camera. The hardware bag includes a full size SD to MicroSD adapter in case you ever need to erase/reformat the MicroSD in a computer with a full size SD card slot.

Since all our outdoor cameras have the PoE feature, for powering the camera you can choose between using the AC adapter or "power over ethernet" (PoE).

Please note that the AC adapter cannot be exposed to moisture. If you use the AC adapter outdoors, it would have to go into an outdoor power outlet with a completely enclosing cover. For example, see "Code Keeper" or similar brands.

If you need more than the 10 ft length of the power cable on the AC adapter, you could skip the AC adapter and instead power the camera with PoE. That would allow you to use inexpensive Cat5e network cable to supply power from up to 300 ft away. Cat5e network cable with the required connectors is available at Home Depot in convenient rolls of 15 ft, 25 ft, 50 ft and 100 ft.

To use PoE you need a PoE power supply (Not included). This could be the $17 PSW4824-POE from L-Com.com or a similar unit from PremierTek (see below).

For wireless networking, the "Data In" port would remain empty, and there would only be a single Cat5e wire from the "Data and Power Out" port going to the camera.

For wired networking, you would add a second Cat5e wire going from the "Data In" port to your router, either directly or through a network switch.

For wired networking you can also use a PoE network switch instead of PoE power supply. Our favorite PoE switch is the Netgear GS108PE. It is more expensive than a single port PoE injector, but can power 4 cameras.

The SCNC3904 retail package includes a weatherproof shell for the cable connectors. When using the camera with the included AC adapter, using this weatherproof shell is entirely optional.

However, when powering the camera with PoE, especially at locations near the ocean, the weatherproof shell should definitely be used to protect the network connector from moisture and corrosion. In fact, please note that warranty coverage is void if the camera is powered by PoE and if the network connector is left exposed to moisture, without use of the weatherproof shell.

Motion Detection or Timed Emails, DropBox or FTP Upload

The camera refers to motion detection as an "alarm". In the camera's "Task Management" menu you can select what you want the camera to do once there is an alarm or once a certain time period has elapsed.

Task 1 "**Email alarm sending**" allows you to set up the details of your email server account and have the camera send you an email with an attached JPEG snapshot. This means the camera can alert you on your cell phone with a picture when it detects motion. You can also set it up to send you pictures automatically every few minutes, or have the camera upload these files to DropBox or an FTP server with tasks 2, 3, and 4 respectively.

One thing to keep in mind when sending pictures to cell phones is that without an unlimited data plan you might incur charges by your cell phone carrier for each picture, and that wrong settings for sensitivity or motion detection area can result in lots of extra emails or DropBox uploads. So we suggest testing it with your phone connected to your Wifi first, before you incur data charges.

The factory default setting for motion detection is a single motion detection window covering the entire visible area. The "**Motion Detection**" menu allows you to designate up to 4 separate windows with individually adjustable sensitivity, however you should keep this menu at default settings until you are more familiar with the more basic setup steps.

Please note that this "**Motion Detection**" menu is entirely optional and is generally not used unless you have very specific requirements to treat motion on some parts of the screen different from other parts. Please see Appendix C for further details on this menu.

The much more important part of the motion detection setup is in the "**Task Management**" menu, specifically the task 1 "**Email alarm sending**"

For automatic emailing you will need both an outgoing email server and one or more receiving email addresses. For the outgoing server we strongly recommend to sign up for a new free Gmail account to be used just by the camera for sending emails. Since that account needs specific settings, it should be separate from your regular email account where you would receive emails.

 Following is an example of a proper configuration for using Gmail as the outbound server. This can be used send email to any receiving email address such as Yahoo, Hotmail, Outlook, or others.

```
Email Alarm Sending

    Snapshot from:          Primary stream    ⌄
    Snapshot duration:      1          seconds (1-3)
    Alarm interval:         1800       seconds (1800-86400)
    Image file name:        PA
    Suffix of file name:    ○ Sequence number  ⦿ Date time  ○ None

    SMTP server name:       smtp.gmail.com
    SMTP server port:       465
    Secure SSL connection:  ⦿ Yes  ○ No
    Authentication:         ⦿ Yes  ○ No
    User name:              yourgmailaddress@gmail.com
    Password:               ●●●●●●●●●●●●●●
    Re-type password:       ●●●●●●●●●●●●●●
    Sender mail address:    yourgmailaddress@gmail.com
    Receiver mail address:  anyotheremail@anywhere.com



    Subject:                Warning from Network Camera  ×
    Message:                See attached picture


                    Apply     Back
```

Note: Your account on Gmail.com needs the following settings: In the **"Forwarding and POP/IMAP"** tab you need **to enable POP & disable IMAP**. In the **"Accounts and Import"** tab, you go to **"Other Google Account settings"** and in the **"Signing in to Google"** section you would disable **"2 step verification"**. IMPORTANT: scroll all the way to the bottom of "**Signing in to Google**" and set **"Access for less secure apps"** to **"Allowed" or "On"**. With some browsers, Google hides the setting, requiring a special link to get to it:

https://www.google.com/settings/security/lesssecureapps

Note that if you have a typo in any of the above information, the camera would have no way to let you know about that. You just won't get emails. To summarize, Gmail requires the following in the camera's email server setup:

- SMTP server name: **smtp.gmail.com**
- Port: **465**
- Authentication: **Yes**
- Secure SSL connection: **Yes**
- Your username _must_ include **@gmail.com**

Other mail servers have their own unique settings and requirements. Some web mail services such as Yahoo can typically not be used for sending unless you subscribe to optional paid subscriptions like Yahoo PLUS. Any email account can be used as a receiving email address, including the same as the sending email. You can also have more than 1 receiving email address, up to 3 total. NOTE: It is easy to have a typo. The SMTP server name never has an @ symbol. On the other hand, email addresses must have the @ symbol.

VERY IMPORTANT: For the gmail account used with the camera, the password must not be longer than 22 characters and must not have any spaces, punctuation, or foreign characters. Upper case and lower case are distinct and must be entered correctly in the camera. To make sure no extra space is added, it's best to type the password rather than cutting and pasting.

For large pictures you'd keep the factory default setting of "Snapshot from" "Primary Stream". For smaller pictures you can select the "Secondary Stream".

For "Image file name" we recommend keeping the default ("PA" for "picture on alarm"). The rest of the generated file name can include time & date or a number. Do not add any file name extension, as .JPG is added automatically.

The "Alarm Interval time" allows you to designate a time (in seconds) during which new emails are suppressed. To avoid a flood of emails and risk having your email account blocked for suspected spamming, this is pre-set to 1800 seconds to prevent additional emails for at least half an hour. If you need very frequent motion detection notifications, you may want to consider using FTP or Dropbox uploads instead of email.

When you are done with choosing settings for the email alarm sending task, you would click on "Apply" to save the settings, then click on "Back" to get back to the "Task Management" menu.

Now if you want motion detection emails to start, check the "Enable" checkbox for the "Email alarm sending" task, and click on "Apply" in this Task Management screen. With the task enabled, you should be getting your first email shortly after you walk in front of the camera. Then you will not be getting additional emails until the "alarm interval time" elapses (half an hour).

Task Management

No.	Enable	Schedule	Task
1	☑	Always ∨	Email_alarm_sending
2	☐	Always ∨	Email_periodic_sending

If you prefer, you can have the pictures uploaded to DropBox or an FTP server instead of an email address. To do this, go to the **"Task Manager"** menu and either click on task 3 **"FTP alarm sending"** or task 4 **"FTP periodic sending"**, depending on whether you want to send images upon motion detection or based on elapsed time such as every few minutes.

Note: Both DropBox and FTP are enabled in the FTP task management menus, and in both cases the setup is very similar to the email task management.

Snapshot From / Duration / Frame Rate / Alarm Interval: These settings are identical to the corresponding settings in the email task management menu.

If you select DropBox in any of the FTP menus, the **"Authorization"** button opens up a new browser tab or window to allow you to enter your DropBox account info. If you don't see the new tab or window, please make sure your browser does not have a popup blocker enabled during this setup.

If you select FTP instead of DropBox, you'll need to fill in the **FTP Server Name** and **Port** fields. Do not add any extra spaces, and do not add ftp:// or anything else in front of the server name or IP. The **FTP server port** is almost always 21.

Authentication: Most FTP servers need a username and password which means "Authentication" should be set to "**Yes**". Make sure the username / password are spelled correctly including all uppercase/lowercase letters. Do not use usernames and passwords with spaces or punctuation, or anything more than 22 characters long.

Remote path: No need to specify a remote path unless you want to keep the files organized into folders. In that case you'd make sure the spelling of your path is identical to the name of the preexisting folder on the server, and that your account has read/write/delete rights for that folder. If in doubt, leave the path totally blank and the files go into your account's default folder.

If you maintain your own web page there is a neat feature available by setting the **"Suffix of file name"** to **"None"**. This allows you to upload a file with the exact same file name every time there is motion. If you then reference that file name in your web page it will always show the latest available picture.

Please note that the menu option for **HTTP task management** servers is not explained here since HTTP servers are only used by network professionals.

The following chapters will show even more possibilities for tasks. For example, you can use motion detection or time periods to initiate the recording of video or snapshots to MicroSD card.

Stream Setup and Recording Options

There are several different ways in which the camera can record video. All methods can be used with or without motion detection.

1) Totally automatic, standalone recording to internal MicroSD card

2) Totally automatic recording to a network drive (NAS, not USB)

3) One-click recording on a Windows PC using Internet Explorer

4) Recording on a PC with software such as BlueIris, LuxRiot, SightHound

5) Recording on a Mac with software such as EvoCam, SecuritySpy

Most customers choose the camera's standalone recording to MicroSD since this option requires no other equipment to be on or even present at the camera location, and requires no software purchases or accessories.

Some customers prefer recording with a computer, even though this would require the computer to remain on at all times without being allowed to go to sleep or standby. This method allows quicker access to recorded files since they are already on the computer without any transfer needed. Also, this is typically preferred when displaying or recording multiple cameras.

For recording, you can generally get good results with the factory default settings in the **"Stream Setup"** menu. However, we recommend reducing the frame rate to 15 fps or 10 fps to stretch the amount of available recording time without too much impact on the video quality. Also we recommend reducing the bit rate from the default 2048K to 1536K or 1024K.

IMPORTANT: If you are planning to use more than 1 task enabled in the task management menu, or if several cameras are being recorded to a computer, or if you plan on continuous live viewing while also recording, or if you are using the "pre-record" function, the frame rate should be lowered to 10 fps on all streams, with a bit rate of 1024K for the primary stream and 256K for the secondary stream. MJPEG quality should always be 50 and snapshot quality should always be 90 for both primary and secondary streams.

Alternately, it is also possible to record from the secondary stream. This is especially useful for the most efficient use of storage capacity when doing continuous recording, and can also be combined with motion detection snapshots so that you have an idea at what times in the continuously recorded video the camera detected any motion.

Recording to built-in Micro-SD card

The SCNC3904 comes with a 16 GB MicroSD card pre-installed and is ready to record. 16 GB gives you plenty of storage space for motion detection recording of an area that is not too busy and doesn't have swaying trees or passing cars.

If you wish to upgrade the card anyway, please note that any new card *must* first be formatted in a PC or Mac with the free software from **www.sdcard.org** and these options: **FORMAT TYPE = FULL , FORMAT SIZE ADJUSTMENT = ON**. This takes about half an hour on a 32 GB card. Cards larger than 32 GB require a Mac for a second formatting step (see page 55). If you don't have a Mac: preformatted 64 GB cards can be purchased from Sharx Security.
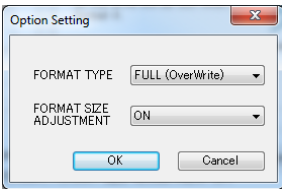
Note: The picture shows the PC version. The Mac version of the formatting software has slightly different wording. You would first click on "Option" to select "**Logical Address Adjustment = YES**" and then you would select "**Overwrite Format**".

The card slot is on the side of indoor cameras, or behind the lens cover of outdoor cameras (see diagram on page 43). When the camera powers up, the "**System**" screen shows the available space, while the "**Storage**" menu allows you to browse the contents. The format option in the Storage menu erases files but is not a substitute for the required full format prior to first use.

The "**Task Management**" menu allows you to enable continuous or motion detection (alarm) recording of video clips or snapshots.

To start recording video with motion detection, all you need to do is to place a checkmark on task #9 in the Task Management menu, and "Apply".

If you like to see available options for this task you can click on the blue underlined "**Record to Storage on alarm**" and this will open the menu shown below. We recommend leaving all options at factory defaults for now, except maybe changing the "Record from" option to "Secondary Stream" if you prefer to use less storage space with medium resolution files. The details of the available streams are explained in a separate chapter "Stream Setup"

The resulting video files are listed in the "**Browse Storage**" menu. Clicking on "Play" for any file will attempt to stream that file from the camera with minimal startup delay. This works only with fast network connections.

"Download" will work even with slow network connections as the entire file is downloaded before playing starts. Then the file will be opened in the media

player application that your computer has associated with the .MOV file type, for example QuickTime player on Macs or the Movies or Windows Media Player on Windows. Older versions of Media Player cannot play the sound. In that case you can install the free Apple Quicktime Player for Windows. Shorter video clips will download much faster.

Do not remove the MicroSD card while recording is active. If any recording task is enabled, you should disable recording and wait 1 minute before removing the card. Errors caused by removal during recording might require reformatting of the MicroSD card in a computer.

To access the MicroSD card slot on outdoor cameras, you may want to wait for a day where there is no rain and very low humidity. Then unscrew the entire front part of the camera. It is easiest to do it if you take the sunshield off first.
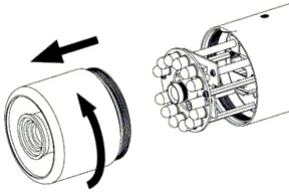
The location of the SCNC3904 MicroSD card slot is shown below:

MicroSD card slot
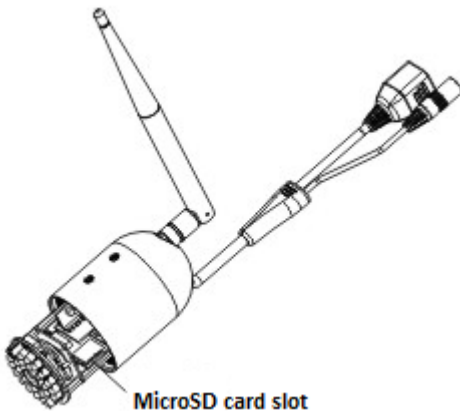
Please be very careful not to touch the lens. The MicroSD slides into the slot and there is a positive "click" when it is locked in place. If it doesn't want to go in effortless it is probably upside down.

The correct orientation of the card is with the contacts facing down and the writing facing up.

When done, please be careful when screwing the front part back on to make sure the threads are engaging nicely. Do not use any tools, hand tight is good enough, and please be sure not to flex the camera mount while doing this.
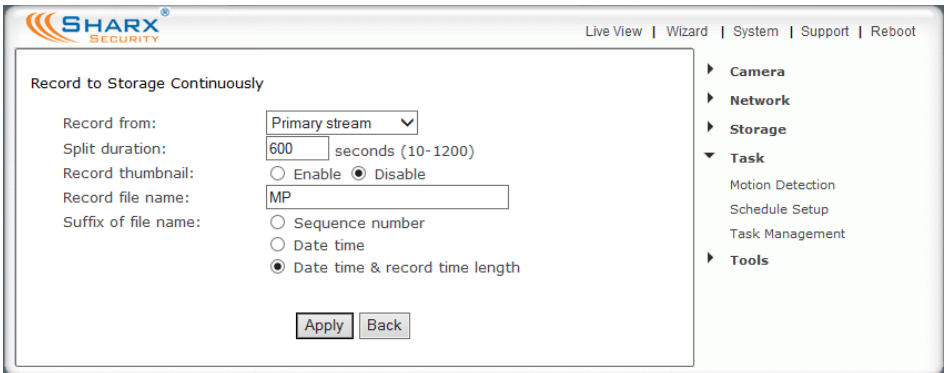
Using the camera as a continuously recording DVR

At the highest settings of video quality, recording can take 0.5 – 1 GB per hour, so the standard 16 GB MicroSD card is typically only used for motion detection recording ("record on alarm"). With lower settings it is also practical to use the camera as a continuously recording DVR (Digital Video Recorder).

For example, if you set up the "**Secondary Stream**" in the camera's "**Stream Setup**" menu to a lower setting such 768 x 432 resolution, a frame rate of 10 fps, and bit rate of 256K, this allows about 5 days with the standard 16 GB card, 3 weeks with an optional 64 GB card, and 6 weeks with a 128 GB card.

Increased H.264/MPEG4 bit rate improves image sharpness while increased frame rate makes motion appear smoother. For continuous recording, a frame rate of no more than 15 fps is recommended.

To enable DVR recording, click on "**Record to storage continuously**" in the Task Management menu. For longer recording times we suggest to change the "**Record from**" setting to the secondary stream. A "split duration" of 600 seconds as shown below will give you files that are 10 minutes long.

Then click on "**Apply**" and "**Back**", then check the checkbox for the "**Record to storage continuously**" Task, and "**Apply**" again to enable the task.
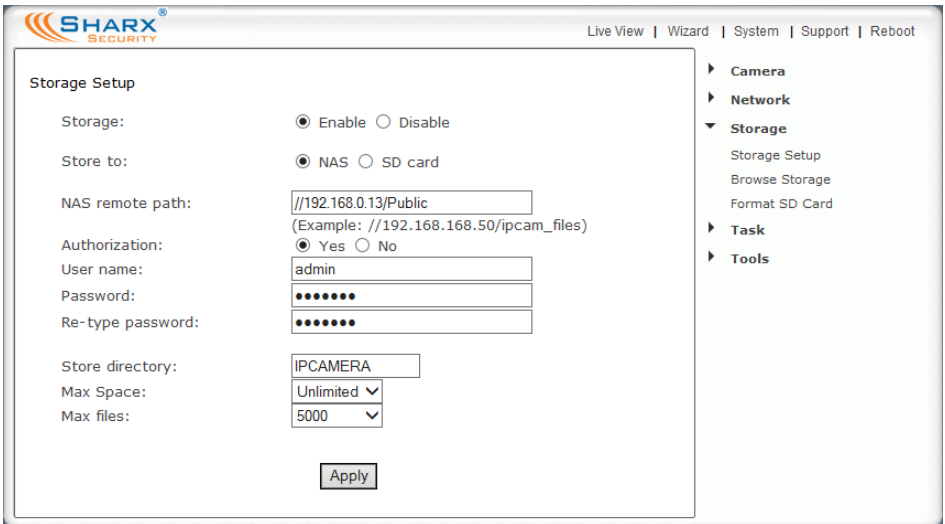
To limit file sizes, video is recorded in individual clips of adjustable size. You can then view your files in the "**Browse Storage**" menu. With a split duration of 600 seconds there will be 6 files per hour. After the MicroSD card is full or the file number limit is reached, the oldest file is automatically deleted.

Alternatively you can also enable recording to a NAS drive as described in the next chapter, giving the camera NVR (Network Video Recorder) functionality.

NAS drive setup

The "**Storage Setup**" submenu allows you to select a NAS (network attached storage) drive instead of MicroSD as the destination for the camera's standalone recording. If NAS is selected you need to make sure your NAS drive has a permanently assigned IP address that does not change after a restart. You also need to know the so-called network "**share**" name for your drive, as well as username and password.

It is very important to use the correct format for specifying the NAS path: **Exactly 2 forward slashes, IP address, 1 slash, and the share name** (without spaces). So the NAS setup screen would be filled in similar to the following:

The share name is the name of the top level folder that a NAS drive shows on the network. You can check it by clicking on the icon for the NAS in your PC's "Network" or "My Network Places" folder, or on a Mac by using Finder, then "Go to…" and "Network" and then clicking on the NAS icon.

In the example on the next page, the drive TC1 has a network share named "disk", and MYBOOKWORLD has the shares "SharxCam1" and "Public". For NAS drives **other** than Apple Time Capsule, **if your share name has spaces in it you need to rename it without spaces**. Each NAS drive has its own menus. Consult your NAS manual for details on creating or renaming network shares. A Time Capsule creates shares automatically based on user accounts.

IMPORTANT: Only specify the share name, not folder names. For example, //192.168.0.13/sharename/foldername would not work.

Network folder as shown on a PC: Network folder as shown on a Mac:
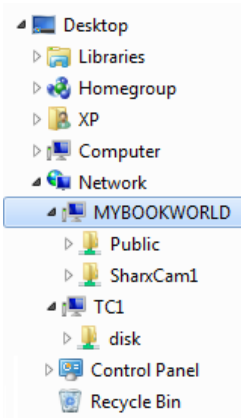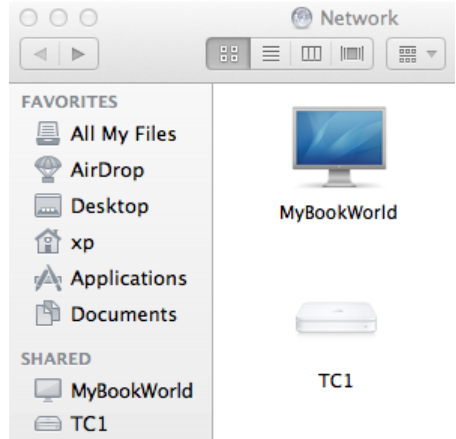
To set up a Time Capsule for use with Sharx Cameras: In Airport Utility, go to the "Disks" icon at the top, then to the File Sharing tab, make sure "Enable File Sharing" is checked. Use "Secure Shared Disks" setting: "With accounts", then configure an account for each camera, for example "SharxCam1". No spaces or punctuation are allowed in the account name or password. Make sure the account has "Sharing Access" of "Read and Write", then update these settings. Next, go to the globe shaped "Internet" icon at the top, click on the TCP/IP tab, and check the IP address of the Time Capsule. Typically the IP address is 10.0.1.1 but can be different if the Time Capsule is in bridge mode.

Go to the camera's "Storage Setup" menu, enable it, select "NAS", then for the NAS remote path enter these things exactly with no extra spaces: two slashes, the Airport's IP address from the previous step, one slash, then the name of the user account you created for the camera. If you followed the example above, the camera's NAS path would be:

NAS remote path: //10.0.1.1/SharxCam1
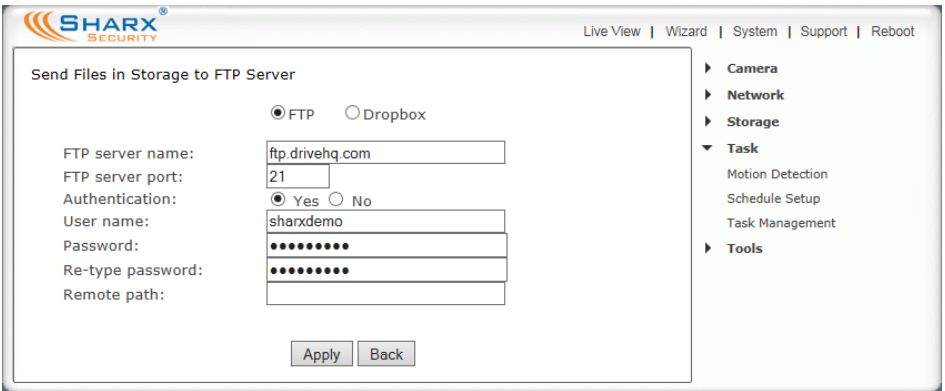
Then click on "Yes" for authorization, enter the username and password for the account you created, "Apply", and after about a minute click on "System" at the top of the camera's settings screen again, and scroll all the way down to the storage section. You should have a NAS status of "Ready" and lots of storage available.

Now you can use "**Record on Alarm**" for motion detection video, "**Continuous Record**", "**Snapshot on Alarm**", or "**Snapshot at Interval**". When the file number limit is reached or storage is full, the oldest files are deleted.

Transferring MicroSD files to DropBox or an FTP server

If you do not have a locally connected NAS (network attached storage) drive but still want to upload your recorded video files to a server, you can do that with the new task management menu "Send files in storage to FTP server". This works with DropBox or online FTP servers such as DriveHQ.com

As with the direct uploads of snapshots described on page 39, you can choose if you want the upload to go DropBox or an FTP server, and you would supply your login information in the same way (i.e. by supplying the FTP server name, username and password, or by selecting DropBox and then clicking the camera's "Authorize" button to add the DropBox specific login information).

 "**Remote Path**" specifies the name of an existing, write-enabled folder on the server. We recommend to keep this completely blank at first. After you see some files being uploaded, you could specify the name of an existing folder, and then the files should go into that folder if there are no typos.

Once successfully transferred, each original file on the MicroSD card is deleted. To prevent files from piling up on the MicroSD card, the rate at which the files can be transferred to your FTP server has to be much faster than the rate at which new files are created, and therefore this feature is generally only useful for motion detection recording. This allows the files to be transferred at times when the camera is not detecting motion and creating new files.

For continuous video you would use settings as shown in the previous chapter to record without FTP transfer. If the camera is multitasking and busy with recording, sending or viewing, there could be interruptions in the recorded audio and video. For best results, enable only the tasks you really need.

Recording Video using a Computer

To record video or snapshots, you'd generally use the camera's own MicroSD or NAS recording methods as described in the previous chapters. This has the advantage that no computer or software is needed, even if you want the camera to transfer the resulting video to DropBox or FTP or cloud servers.

There are cases when you might prefer to record video using a computer, for example if you have many cameras and want to display and record them all together as a group. Fortunately there are some really nice software packages that support our cameras.

For PCs in residential applications, BlueIris from www.blueirissoftware.com works well for up to 16 cameras and is a great deal at just $59.95. Stepping up to business applications with multiple servers and hundreds of cameras at different locations, LuxRiot from www.luxriot.com is the professional's choice. For Mac users we recommend the $30 EvoCam from www.evological.com.

Below are some screenshots and hints showing how to configure the 2 most popular software packages from other companies for Sharx Security cameras:

To configure **BlueIris** software, you would use the menu to add a new camera and select "**Sharx H.264 RTSP**" as the "**Make/Model**", and then you would make sure that the Media/video/RTSP port is set to the same value as the HTTP port, usually 80 for any local camera or 8150 for the first remote camera.

To configure **LuxRiot** software, you would not use Sharx Security as the manufacturer since LuxRiot has not been updated yet for our new cameras.

Instead, you would select "**Generic**" as the manufacturer and "**RTSP Compatible**" for camera type and then configure it as follows:

In the "**Access**" tab you'd add the IP address and port, as well as the username and password. The port is generally 80 for all cameras on your own network, and 8150 for the first remote camera.

Then in the **RTSP** tab you would uncheck "Use default port" since that generally uses the wrong value 554. Instead, you'd add the exact same port as you used on the "**Access**" tab, generally 80 for all local cameras and 8150 for the first remote camera.

The option "**RTP over TCP**" should be checked.

There are 2 "**Path**" fields for the session description file, one for high resolution and one for low resolution.

In the "**High**" field you would enter: **/live/0/h264.sdp**
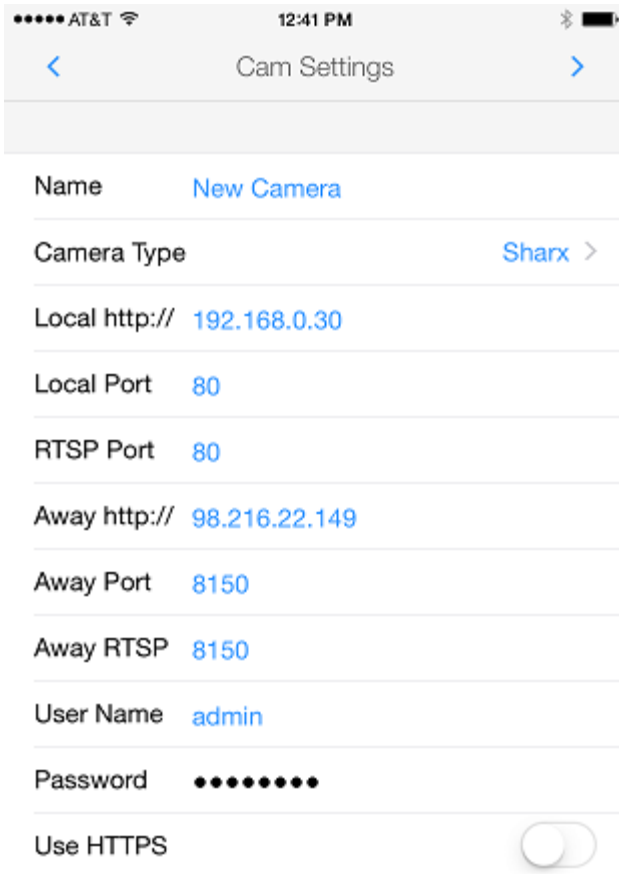
The "**Low**" field can remain blank or: **/live/1/h264.sdp**

iPhone Apps

All Sharx VIPcella series cameras can be viewed directly in Safari which is available on all iPhone, iPad, iPod Touch devices. No app is needed, and Safari allows very nice video with audio on iPhones and iPads. It is very easy to bookmark the local and remote IP addresses of your cameras to the Safari "Favorites", and then you can view your camera simply by clicking on the book shaped icon next to the Safari address bar and clicking on the saved bookmark.

Should you prefer to use an app, our current top recommendation is the free app called "**MobiLinc Cam Viewer**" by Mobile Integrated Solutions, LLC.

Setup is straightforward, just select "Sharx" as the vendor and enter both your camera's local IP address and external IP address. The local port is usually 80 while the away port is 8150 for the first camera. MobiLinc likes to fill in the RTSP port with the default value of 554 but this is wrong. The RTSP port is always set to the same as main port, i.e. 80 or 8150 respectively, as shown in the example below. Of course you would use your own camera's IP addresses:

Android Apps

Current Android devices such as Google Nexus or Samsung Galaxy can view our cameras directly in the browser, without any app needed.

If you prefer to use apps, you could try the free version of **tinyCam.**

For setup, be sure to select "**Sharx Security**" for "**Camera vendor**" and "**SCNC3905**" for "**Camera model**". Then add your camera's IP address in the "**Hostname or IP address**" field, without any extra characters. For example, a local camera would have only the local IP address, for example: 192.168.0.30
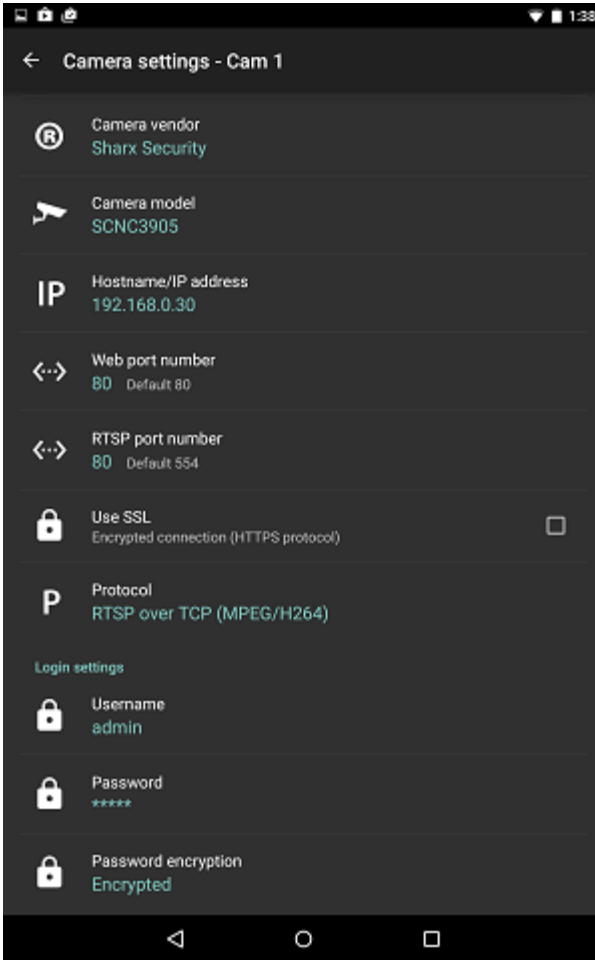
For a remote camera you can add either the external IP address, or you can use your No-IP hostname if you have set one up for your camera.

Then skip ahead to "**Protocol**" and select "**RTSP over TCP**".

Now you can add both the "**Web port number**" and the "**RTSP port number**", both of which would be set to the same value:

For local cameras both of these ports are usually 80 (not 554), and for the first remote camera the value is usually 8150

Additional remote cameras would have the same IP address or hostname. Only the port number would be different. For example, the second camera would have 8151, the third camera would have 8152, etc.

Page 52

Audio/Video Stream Reference

The camera supports multiple simultaneous video streams that can be configured with their own resolution, frame rate, and bit rate settings. Entering through the main login screen automatically activates the highest resolution video stream, called the Primary Stream.

For access to specific types of audio or video encoding, you can bypass the main login screen and go directly to a stream with the desired protocol and encoding. The full list is accessible by clicking on the blue underlined "**Primary Stream**", "**Secondary Stream**", or "**Mobile Stream**" in the Stream Setup page.
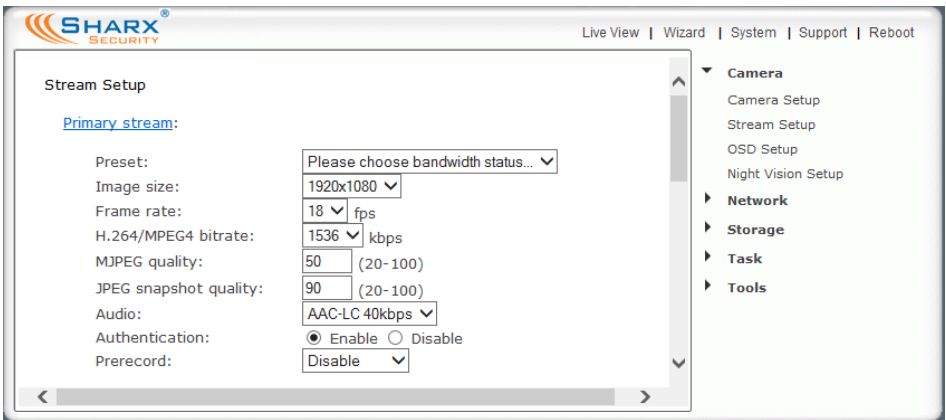
For example, clicking on the blue underlined "**Primary Stream**" will result in:

Primary Stream List

Intranet stream URL	
RTSP H.264 stream:	rtsp://192.168.0.24:80/live/0/h264.sdp
RTSP MPEG4 stream:	rtsp://192.168.0.24:80/live/0/mpeg4.sdp
RTSP MJPEG stream:	rtsp://192.168.0.24:80/live/0/mjpeg.sdp
RTSP audio stream:	rtsp://192.168.0.24:80/live/0/audio.sdp
HTTP M3U8 stream:	http://192.168.0.24:80/live/0/h264.m3u8
HTTP MJPEG stream:	http://192.168.0.24:80/live/0/mjpeg.jpg
HTTP snapshot image:	http://192.168.0.24:80/live/0/jpeg.jpg
RTMP H.264 stream:	rtmp://192.168.0.24:80/live/0/h264.flv

You'll notice that some entries start with "RTSP:" instead of "HTTP:". This is not a typo. **RTSP streams can be played by Apple QuickTime Player or the VLC Media player from www.videolan.org**. The RTMP stream can be played with **JWPlayer** or **Adobe Flash Player** embedded in a web site. The HTTP M3U8 stream can be played by iPhone, iPad, Mac OSX, and recent Android versions.

Resetting the Camera back to Factory Settings
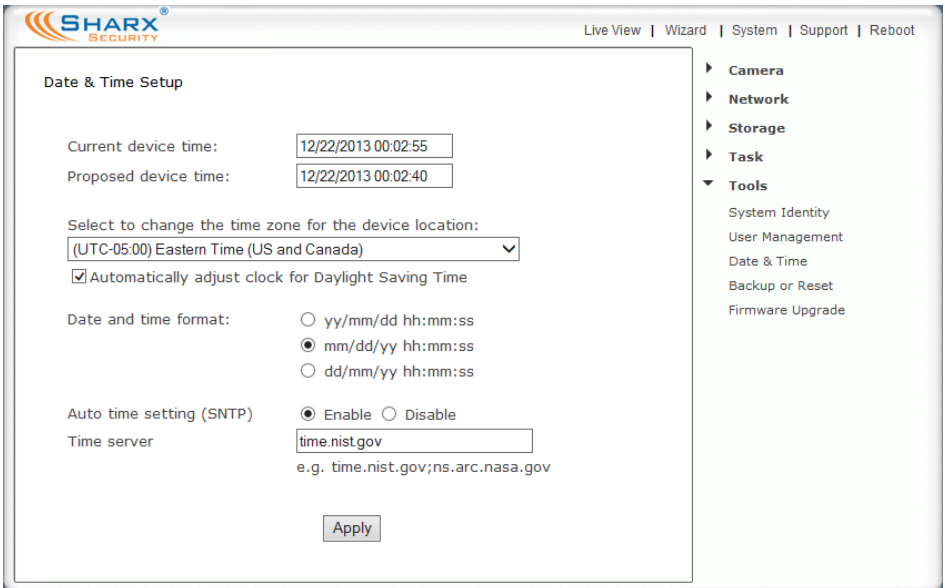
If you ever forget your admin password or have any other reason to want to remove all your settings and reset the camera to the factory defaults:

1) Make sure the camera is powered up

2) Find the SCNC3904 reset button at the bottom of the camera. It looks like a small white eraser head. In general it is easier to use the software reset function in the "Backup or Reset" menu.

3) **Press and hold the reset button for 10-15 seconds.** You'll see the power light go off twice in the next 45 seconds. This indicates that the reset to factory settings is in progress.

After the restart, the camera will be at factory settings. This means the username and password will both be "admin" again, and all previous wireless network info is wiped out and replaced with the factory default as well.

Setting the Time and Time Zone

The camera can check or correct its time automatically if the camera has internet access. You'll need to select your time zone in the Date & Time menu:

SPECIFICATIONS	(subject to change without notice)
Camera	
Imaging Device	New generation CMOS sensor with enhanced night vision
MegaPixels	2 MegaPixels
White Balance/Exposure	Fully Automatic, with manual override and fine tuning available if desired
Viewing Angle	SCNC3904 (standard version) 55° SCNC3904-WIDE (wide angle version): 72°
Focal Length	SCNC3904: 6mm SCNC3904-WIDE: 4mm
Lens Aperture	F2.0
Min.Ilumination	All models can see in total darkness (0 Lux) with IR
Infrared LEDs	24 medium power LEDs Automatic IR filter for excellent daytime colors on all current models
Network	
Image compression	H.264, MPEG4, JPEG, MJPEG, 3GPP
Image resolution	1920 x 1080 (1080P) and various lower resolutions
Max. frame rate	30 fps viewing / 20 fps recording @ 1280 x 720 (720P) 18 fps viewing / 15 fps recording @ 1920 x 1080 (1080P)
Audio compression	AAC (40/32/24/16Kbps)
Built-in microphone	Electret Condenser Microphone
Simultaneous viewers	Up to 4 depending on settings and available internet upload bandwidth
Authentication	Username/Password. Selectable "Digest Access" or "Basic" Authentication
Network protocols	TCP,UDP,IP,ARP,ICMP,DHCP,DNS,HTTP,FTP,SMTP,NTP,UPnP,DDNS,RTSP,RTP
Stream types	HTTP, HLS, FLV, RTSP/RTP/RTCP, 3GPP
Network connection	Ethernet (10BASE-T/100BASE-TX) and 802.3af PoE
Wireless LAN	
Wireless technology	IEEE 802.11 b/g/n, 2.4 Ghz
Security	WEP (64/128 bit, Hex/Ascii), WPA-PSK (TKIP), WPA2-PSK (AES)
General	
Power requirements	DC 12V 1 Amp (international AC adapter included) alternate power source: PoE 802.3af
Power consumption	Up to 8 W at night with IR LEDs on, up to 5 W daytime with IR LEDs off
Operating temperature	-20 to +60 °C (-4 to +140 °F)
Operating humidity	0% to 100% RH (weatherproof)
Dimensions	2.25" diameter x 5" long (57 mm x 125 mm)
Weight	15 oz / 425 g (Main Body with Sunshade)
Supplied accessories	AC adapter, Cat5e cable, antenna, wall/ceiling mount, sunshade, Weatherproof shell for protection of cable connectors
PC system requirements	
Operating system	Windows 7-10, Macintosh OSX Mountain Lion – El Capitan, Linux
Processor	Intel Core 2, Core i3 – i7 (Multiple cameras require faster processor)
Memory	4 GB RAM Minimum
Web browser	Microsoft Internet Explorer Version 9 - 11, Edge, Chrome, Firefox, Safari
Memory Card	MIcroSD and MicroSDHC capacities of 4 GB – 128 GB are supported Speed Class: Class 10 or better required to meet specified recording fps NOTE: All replacement MicroSD cards **must** be formatted in a computer using software from www.sdcard.org/downloads and "full format" and "size adjustment (or logical addressing)" = ON options. Cards above 32 GB also require a second formatting step to adjust the file system from ExFAT to FAT. Since this step is required and can only be done with "Disk Utility" on a Mac, do not purchase 64 GB or 128 GB cards if you do not have access to a Mac.

Glossary: A quick Review of Networking Terminology

To participate in a computer network, each device needs an "Internet Protocol" address that is unique on that network. This **IP address** consists of 4 groups of numbers separated by periods. For example: 192.168.0.2

IP addresses are assigned to a device either automatically by the **router** or manually by a person who is setting up the network. The router is the device that is managing the addresses and the flow of data between those addresses on your network. Sometimes the routing function is not provided by a separate device and is built into your cable modem or DSL modem.

When you first plug the camera into your router with the network cable, the camera asks the router to get a valid IP address, and the router provides the next available IP address on the local network. With "**local network**" or **LAN** we're referring to your own home or business network. On the other hand, the term **WAN** or "**Wide Area Network**" refers to the global internet.

Your router is sometimes also called a gateway because it is like a gateway from your own local network to the internet. Unless you have an all-in-one combination of modem and router you'll probably see that your router has one network jack marked WAN which connects to the cable or DSL modem and a set of 2 or 4 jacks marked LAN for your local network devices.

Your router will have 2 IP addresses of its own, a WAN IP address that identifies it on the internet and a LAN IP address that identifies it on your local network. The LAN IP addresses often start with 192.168 or 10.0

From any computer on your network it is easy to find the WAN IP address of your router just by opening a browser and going to www.checkip.org

Since your own private network devices including your camera are not directly visible from the internet, for remote access you would typically use your router's WAN IP address together with some instructions to your router to forward the requests from the internet to your camera.

The messages going back and forth between the camera and the router regarding the initial IP address are called **DHCP** for "Dynamic Host Configuration Protocol".

Each device also has a unique hardware address that is called a **MAC address**. This MAC address is unrelated to Macintosh computers. What's special about this hardware address is that it is totally unique to each network device.

Appendix A: Wireless setup instructions without Cat5

We have received inquiries from customers with no available wired network jack for the camera's initial configuration. Or sometimes a camera is inadvertently mounted before wireless setup.

While we don't recommend this, it is still possible to configure the camera without an initial wired connection using the following procedure.

1) Temporarily rename your router's Wifi network name (SSID) to:

    wirelessnc

    Also turn off all wireless security, i.e. no passwords and no MAC filtering. It is important to have the SSID all lower case and without extra spaces. Then connect to this Wifi network with your laptop.

2) Power up the camera and wait about 1 minute… the camera should connect to your Wifi and you should be able to access it using the IP address that you reserved for it. If you did not previously reserve an IP address for the camera, you should see the camera's MAC address and device name in your router's list of attached devices (DHCP client list). Unfortunately Apple Airport routers no longer have the DHCP client list, so Airport users would need to know the camera's MAC address and reserve an IP address as shown in the "Mac Quickstart" chapter.

3) From the main login page with "Enter" and "Setting", log in directly to the camera's "Settings" and go to the camera's wireless setup menu, but do NOT use the "search" function.

    Type the exact SSID that you had before the change in step 1, and type the exact password that you wish to use. Double check it for correct spelling. Then select the correct password type, usually WPA2 with AES encryption, or WPA with TKIP. After double checking everything one more time, click "Apply". The camera will now stop responding since the camera and router's password info are not the same.

4) Now set your Wifi SSID back to the exact same spelling as you entered into the camera's SSID field, and make sure the password and security mode are also exactly the same. Then update and restart your Wifi network. Now the camera and router once again have matching wireless network info and the camera will respond again. You can now proceed with any remaining setup of the camera.

Appendix B: Setup instructions for ATT (2Wire) Router

On the ATT/2Wire 2701HG and similar routers we found that UPnP does not work. For access from the internet you need to log in to the router. ATT usually has the IP address of the router configured to http://192.168.1.254 and the password is usually on a sticker on the bottom of the router. Go to the firewall menu, which has a section for "Hosted Applications" as shown below:

First click on the blue underlined link at the bottom "**Add a new user defined application**". That's 2wire's terminology for port forwarding. 2 applications need to be defined:

The first "application" should be named Cam1HTTP. The public TCP port range is 8150 to 8150 and the "map to host port" is 80. All other settings should be unchanged. The second application should be named Cam1RTP. The public UDP port range is 30000-30001 and the "map to host port" is 30000.

After these 2 applications are defined, you select your camera in the drop down box titled "Choose the computer…" and click on "Allow individual applications. Then add the 2 applications that you defined. You see that they are moved into the box on the right and are therefore active for the selected device. Then you save the settings and restart your router.

For the next camera, you call the first application Cam2HTTP and use public TCP port 8151 while still using "map to host" port 80. The second application would be Cam2RTP with UDP ports 30002-30003 and map-to-host port 30002.

Appendix C: Motion Detection Fine Tuning and Adjustment

After selecting "motion detection" from the main settings screen, depending on your browser you may need to click on OK for installing an ActiveX, or you may need to install the Adobe Flash Player plug-in. Then in most cases you will need to expand the size of the browser window towards the right to see the complete motion detection screen.

The factory default setting is that one single motion window covers the entire viewing area. Sometimes that results in motion detection from objects that should be ignored, for example a swaying tree. In that case, it's best to reduce the size of the motion window so that areas that should not trigger detection would not be covered by any motion window. To cover odd shaped areas you can enable more than one motion window. Each window can have individually adjustable sensitivity and threshold. Windows should not overlap.

In general, motion detection works by comparing the current video frame with the averages of the previous video frames. Any difference is considered to be motion, and the sensitivity adjustment can be used to make the camera more aware or less aware of small amounts of motion.
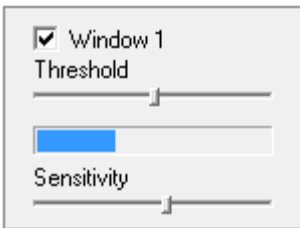
With the ActiveX or Flash plugin, you can see a moving blue indicator for motion: When there is motion, the blue level appears near the sensitivity and threshold adjustment sliders. More blue means more motion. To trigger an alarm (and hence send out emails or record or upload to an FTP server etc) the detected amount of motion needs to be larger than the threshold setting. If the blue level does not reach the threshold setting the motion is ignored.

To reduce the chance of false alarms you would increase the threshold (move threshold slider to right) or decrease sensitivity (move sensitivity slider to left).

Typically, you would just observe the the camera through this motion detection menu and make adjustments to threshold, sensitivity, and motion windows until you're happy with the results. Careful: After each apply, please wait at least 10 seconds before clicking apply again. Since it takes time for the camera to save settings, rapidly repeated "apply" can confuse the camera.

Please note that it does not make sense to define windows if the camera is not mounted securely. Any camera movement shifts or invalidates all windows.

Appendix D: Known issues

1. If you use Internet Explorer: Windows 7 - 8 have no problem with the signed Sharx Security ActiveX. Windows 8.1 issues warnings that can be ignored.

2. If you use Gmail for motion detection and send a very large number of emails in a short time, Google may suspect that you are sending spam and may suspend or block your account. Use the schedule feature to send alerts only when you really want them, and use the interval time to suppress new emails for a given amount of time. We recommend setting the "**Alarm Interval Time**" setting to 900 seconds (15 min)

3. Files recorded by the camera on MicroSD or NAS are in Apple QuickTime MOV format. On a PC we recommend to download and install the latest Apple QuickTime Player for best playback of the files with video + audio. Another alternative is installing the free VLC media player from www.videolan.org

4. Even though there is an option to select a larger number of files on the MicroSD, we recommend keeping the factory default setting of 5000 files. Never change the file number limit while recording is in progress. That might cause errors, requiring reformat of the MicroSD

5. LinkSys routers have a factory default setting in the firewall menu called "Filter Anonymous Internet Requests". The purpose of this setting is to prevent access to any of your network devices from the internet. Therefore if you want to be able to access your camera from the internet you would have to uncheck this option.

6. Some wireless routers or access points have a feature called "guest network" or "wireless client isolation". These features are designed to prevent access from one wireless device to another and are therefore this would be incompatible with the idea of using a wireless camera.

7. Among all the wireless routers we tested, a few specific older models seem to have trouble with wireless connections: LinkSys WRT120N, WRT160N and WRT300N, 2wire 2701HG, Netgear WNDR3700. We recommend upgrading to a newer b/g/n router. All routers should be updated to the latest factory firmware. We do not support alternative firmware such as Tomato, DD-WRT, or OpenWRT.

Appendix F: Suggestions for effective motion detection

We're working on it, but currently consumer cameras are not yet smart enough to recognize if motion is actually caused by a person, even if you followed Appendix C to fine tune motion detection windows and settings.

Generally motion detection is more intended as a tool to reduce boring recording footage where nothing is changing, rather than an urgent call to action every time the camera detects something. Still, it might be interesting to check the details of what led up to a motion detection event.

One way is to enable continuous recording from the secondary stream (as described on page 45) together with motion detection snapshots recorded to MicroSD or emailed or uploaded to DropBox. That way, the motion detection snapshots can indicate where in the continuous recording there might be something worth looking at, including what happened before and after.

Another way to achieve this is with the new "**pre-record**" feature that can be enabled in the camera's stream setup menu. This adds the selected number of seconds prior to the motion event in the "record on alarm" footage.

If you find a lot of motion detection events caused by insects, this cannot be fixed by adjusting threshold/sensitivity settings since a tiny bug up close to the lens appears bigger to the camera than a person at normal distances.

Instead, if the insects are more than just a short term seasonal nuisance in your area, we have these suggestions:

➢ Place inexpensive ($3 - $5) solar LED garden lights near the cameras yet out of the field of view. Most insects are far more attracted to the brilliant bluish white of the solar LEDs than the dull red glow of the IR

➢ An inexpensive ($20 and up) external IR illuminator placed 6 – 10 ft away from the camera would allow you to turn off the camera's own IR LEDs, and that way there would be no attraction at all for the bugs, and no IR light reflecting directly off the bugs back into the lens

➢ For outdoor model SCNC3905 only: The alarm connector described in Appendix E can also be used for the connection of a special dual tech motion sensor. It uses microwaves like a police radar gun to detect moving objects and even uses an IR body heat detector to exclude pets or small animals under 80 lbs. For professional applications, these are available by special order from Sharx Security for under $100

Ready to go far beyond HD to Ultra-Resolution Cameras?

Sharx Security is at the forefront of network camera innovation and quality.

Available to system integrators and installers since 2015, our newest line of Ultra-Resolution cameras includes the **HDNC6301** day/night model with **2048 x 1536 (3MP)** resolution as well as the daytime-only **HDNC5501** with an astounding **2592 x 1920 (5MP)** of live video or snapshot resolution.

Made in USA, these professional models deliver absolutely razor-sharp video or snapshots. Use these cameras with **LuxRiot** software for high end security applications. With **SebecTec** time-lapse software these cameras are perfect for weather enthusiasts. And when used with re-streaming servers it is also finally possible to have public webcams with ultra-definition resolution.

Beta-test sites are eligible for significant discounts. Contact us for details!

Contact us

If you encounter any problems, do not return product to the store

If you have any questions please send us an email: info@sharxsecurity.com

If you purchased this product in new condition from an authorized retailer in the USA, and if you have residential cable or fiber internet service with a current Netgear, Dlink , Asus, LinkSys, FIOS or Apple router, you are eligible for priority email technical support and up to 60 minutes of free US based phone support during the first 90 days after your purchase.

For DSL internet connections, and for support after the initial 90 days, we offer several paid support options. This includes per-incident options for specific issues as well as per hour options for general support. All our support options are for the cameras only. It is assumed you already have a reliable wired or wireless network in place. We do not support satellite internet.

To register you for support we only need your camera's MAC address and the date of purchase. The MAC address can be found on the sticker on the back of indoor cameras, or on a tag on the cable of outdoor cameras.

Please note that remote access to your camera may require a few settings changes in your router. Unfortunately we cannot help with this task if you do not have the password for your own router. Also please keep in mind that with the very low cost of current generation routers it might be more cost effective to purchase a new router than to pay for support on a very old router.

The NVG589 router commonly used with ATT/uVerse does not support more than one camera reliably. If you have that specific router model, you will need to purchase an additional $29.95 or better router from one of the above listed brands before multiple cameras can work for remote access.

Sharx Security and the Sharx Security logo are US and internationally registered trademarks, and VIPcella is a trademark of Sharx Security, Inc.