SHARX SECURITY INC.

WIRED/WIRELESS IP NETWORK CAMERA USER GUIDE

New 2012 series featuring:

Wireless b/g/n networking
MicroSD and NAS recording

V*IPcella*™ series cell phone enabled IP cameras

SCNC2606, SCNC2607, SCNC2700, SCNC3605,SCNC3606

Introduction

Congratulations! You just purchased one of the finest IP network cameras currently available, and this new version can record to a MicroSD memory card

Using a Mac or PC you can view high quality live streaming video with audio direct from the camera. It is excellent for applications such as a baby monitor, nanny cam, pet cam, security & surveillance, remote observation, elder and patient care as well as limited video conferencing or event broadcasting.

The camera also supports mobile viewing of live video or pictures using a web enabled cell phone such as iPhone, BlackBerry, Droid, SonyEricsson, or similar.

Many common usage scenarios are handled directly by the camera's built in web server without the need for 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 WNR2000, LinkSys E1200, Dlink DIR-655. Older routers and some models provided by internet service providers may require some manual setup steps to enable remote viewing. Current Apple Airport routers are fully supported by Sharx 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 online servers using the FTP protocol.

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

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 or Dlink are perfectly fine as long as your router is upgraded with the latest firmware available from the manufacturer. In fact, expensive routers that have too many nonstandard enhancements can often be less desirable than the basic 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.

Contents

Pre-requisites and Setup Overview

This manual applies to all the 2011/2012 series Sharx Security VIPcella™ cameras, which includes the **SCNC2606, SCNC2607, SCNC2700, SCNC3605 and SCNC3606 models.** Besides the camera, you only need:

- **PC, Mac, or Linux computer with internet browser.** The computer is only required for initial setup. 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, you need a **MicroSD or MicroSDHC memory card** from 1 to 16 GB capacity. This card is pre-installed in all outdoor models but **not** included with indoor models.

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.

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 many 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 server setup:** required if you want motion detection emails

- **Stream setup:** required 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 Cat5 network cable that can be used to connect the camera to one of the LAN jacks of your router. Then connect the included AC adapter to the camera and to power. Different camera models may use different voltages so be sure not to switch AC adapters. For all wireless models you should connect the 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.

For outdoor models SCNC3605N / SCNC3606 with connection box:

The cable from the camera connects to the box first. For testing and setup it is not required to tighten the silver lock ring.

The AC adapter also connects to the box. A small green light shows if the box has power. Then you connect the Cat5 cable from the box to the router. The other connections are optional (see Appendix)

On indoor models the camera's power light will come on within a few seconds and turn red/orange if the Cat5 connection is ok. Outdoor cameras purposely do not have a visible power light but you can check the link light on your router to see if the camera is powered up and communicating with the router.

On the SCNC2607 / 2607W you should remove the clear plastic film that is protecting the lens cover. For clearest video never touch the lens.

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 the 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, Vista, or XP, or proceed to **Generic Quickstart** for Mac computers without Airport or for Linux and other platforms.

Mac Quickstart

This Quickstart section applies to the most common configuration for Mac users: You have an Apple Airport (Extreme or Time Capsule), and your Airport is directly connected to a standard, non routing DSL or cable modem.

In this section you will be interacting mostly with the **Airport Utility 5.6**. Please note that the Airport Utility (and this Quickstart section) does not apply if you do not have an Apple Airport router. In that case, go to Generic Quickstart.

Start the Airport Utility by clicking on its icon in your Mac's **Utilities** folder. If you do not have Airport Utility 5.6 you can download it from Apple.com. If you already have version 6.0 on your Mac, that's ok, both version 5.6 and 6.0 can co-exist on the same Mac. Version 6.0 is simplified for easy reference but cannot be used for setup, so you cannot proceed until you have version 5.6

Now select your Airport by highlighting its picture on the left. Click on "**Manual Setup**" and enter the Airport password if needed, and you should now see the Airport Utility summary screen. Let's verify a few things:

1) The version of the Airport firmware should be 7.6.1 or later if you have a current generation Airport. Unfortunately Apple does not provide firmware updates for the earliest Airports. Those could be used with Sharx cameras but require manual IP address setup (see page 24)

2) The **"Wireless Mode**" should be **"Create a Wireless Network**".

3) Click on the globe shaped icon on top, then look at the bottom of the menu for the **"Connection Sharing**" menu. This Quickstart chapter assumes you have: **"Share a Public IP Address**". If you have "Bridge Mode (Off)" it means you have another router on your network that you may need to eliminate or place into bridge mode before you can have your Airport in **"Share a Public IP address**" mode.

With your camera powered up and connected to the Airport, it is ready to use as soon as you look up the IP address as follows:

Click on the white/blue Airport icon at the top and select the "**Summary**" tab. Near the bottom of the summary page, click on "**Wireless Clients**". The individual entries on this summary page may not look like clickable buttons, but most are. A click on the words "**Wireless Clients**" brings you to a screen that has 3 tabs. Click on the "**DHCP Clients**" tab and you'll see a list of devices with their MAC addresses and IP addresses.

One of these entries will be your Sharx camera. You can tell by comparing the MAC address to the sticker on the back of the camera (or tag on the cable).

You could start using your camera immediately using the IP address. Just add http:// in front of it and open it in a browser, such as http://10.0.1.3

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

In general it is best to reserve the IP address to your camera so that you can bookmark the IP address without worry about unexpected changes.

Still assuming that your Airport's "**Connection Sharing**" is set to "**Share a public IP address**", click on the Internet icon on top. Then select the DHCP tab. If you have a new generation Airport you will see a "**DHCP reservations**" box. Click on the **+ (add)** button below this box and enter a description for your camera, such as "SharxCam1", and select "**Reserve by Mac Address**".

Then click on "**Continue**" and enter the MAC address shown on the back of your camera. 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.

Usually an IP address is pre-filled, but do **not** use it. Instead, use the same IP address for your camera as you saw earlier in the "DHCP clients" tab.

Make sure that the last group of digits for this IP address does not end in 1 or 254 since those addresses are usually reserved. Click "**Done**", and you should have the entry in the "**DHCP reservations**". Click "**Update**" to restart.

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.

With older generation Airports the IP address reservation feature is missing in the Airport Utility, however the Sharx camera can be set up for a fixed local IP address using the camera's own TCP/IP setup menu (see page 24).

Next you will probably want to set up the wireless connection. To prepare your Airport for easiest and most reliable connection to a Sharx camera, check the following settings using the Airport Utility:

1. For Airport Extreme or Time Capsule make sure "**Use Wide Channels**" is OFF in the W**ireless Options** "**Advanced…**" menu. We recommend that "**Wireless Channel**" is either 1, 6, or 11 instead of **"Automatic"**

2. On new generation Airports it is recommended to set **"Wireless Security**" to **"WPA2 Personal**". On the camera, this corresponds to Security Mode: **"WPA2-PSK**" with the Encryption Type: **"AES**"

   The older generation 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 or WPA2 security, make sure your wireless password is between 8 and 63 characters and does not contain apostrophes ` ' " . 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 "MAC Address Access Control" feature in the Airport Utility, then you will need to add the camera's MAC address to the allowed list.

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 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.

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, or Dlink 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 routers 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 a pop up window or icon to let you know that a new device has been found. The popup window shows the complete local IP address for the camera. Or, it could be that your camera is automatically discovered by your computer and is shown in the list of attached network devices. On Windows XP this list is called "**My Network Places**". On Vista and Windows 7 it is just called "**Network**".

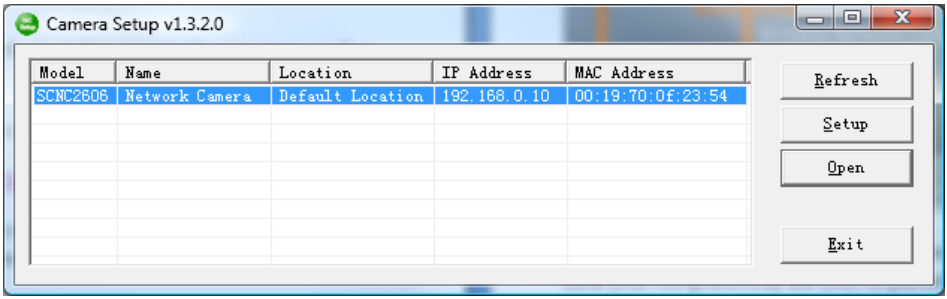
However, some PCs and routers do not have the **UPnP** Universal Plug-and-Play feature enabled. In following we will show alternate ways to find the address that your router has assigned to the camera.

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 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 on the CD called **CameraSetup**. If you install this program on your PC with Windows 7, Vista, or XP, it will tell you the addresses of all current generation 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 number into your browser (with 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 decode the MPEG4 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 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.

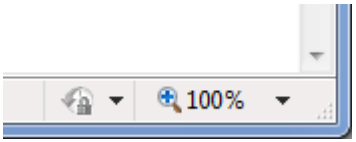
NOTE: If the camera shows video but also displays the message "Connecting, waiting…", close Internet Explorer and wait a couple of minutes for the camera to obtain current time from an internet time server and restart itself.

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 7 – 10. (For use with Safari, Firefox or Chrome please see page 32)

If you find that your Internet Explorer window looks oddly shifted, please check the zoom level / magnification icon at the bottom right of the Internet Explorer window. It should be at 100% for proper viewing of the camera since Internet Explorer can only zoom text and graphics but not a live video stream.



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 Internet Explorer Tools menu, 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 you are running the 64 bit version of Windows 7, and if your computer has separate icons for the standard Internet Explorer and the 64 bit Internet Explorer, be sure to use the standard icon so that you are not starting the 64 bit-only version of Internet Explorer.

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, which is 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 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".

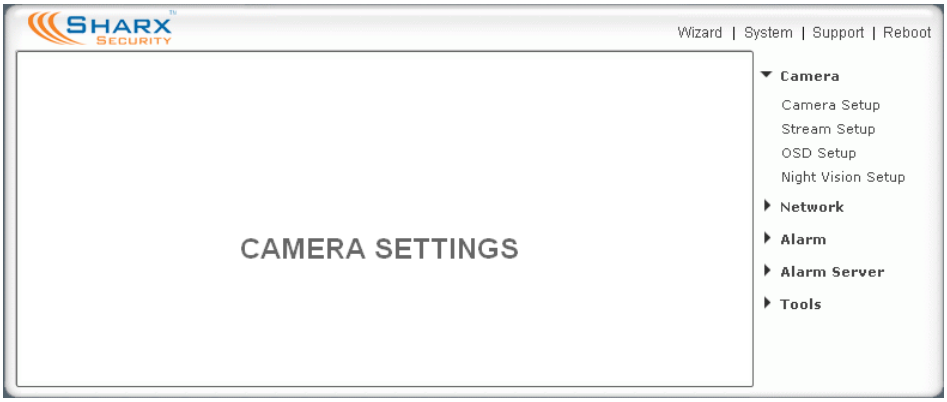
To summarize: **If you can find your router's address reservation menu, you should use it now to lock the camera's IP address in the router. If you cannot find your router's address reservation menu, you would set up the camera's IP address manually, but do not try both methods at the same time.**

Wifi Wireless Setup

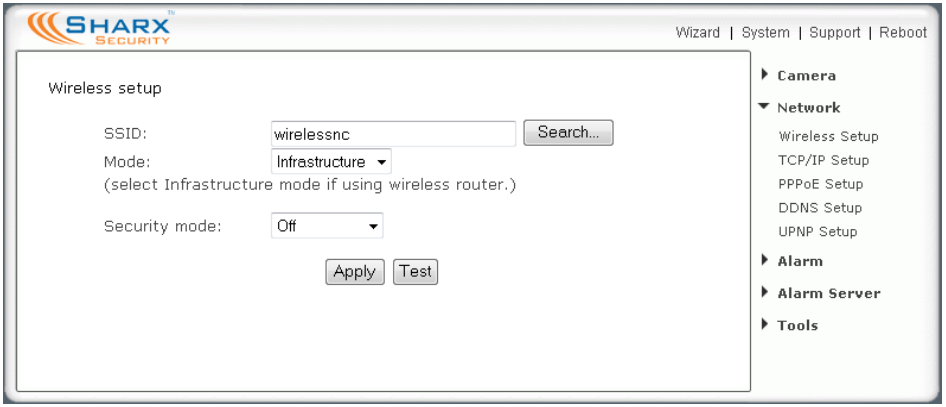
Most likely your wireless network was set up with a password (also known as wireless key). If you don't remember it, you can check your router's wireless setup menu or ask the person who set up your wireless network.

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.

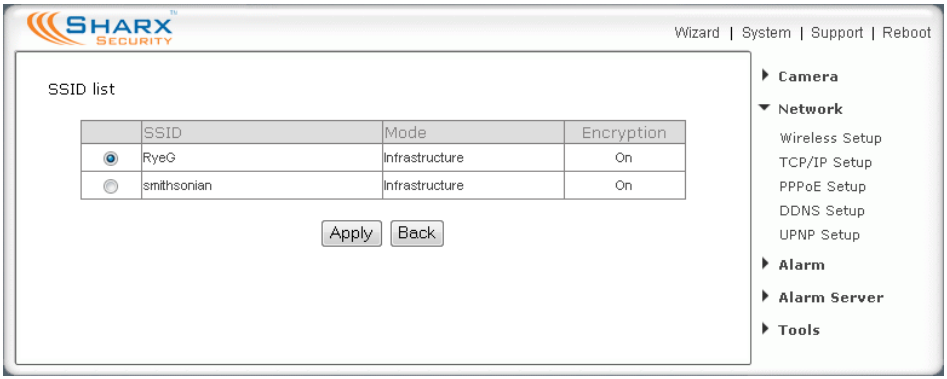
Clicking on "Setting" from the main camera login screen will get you to this:



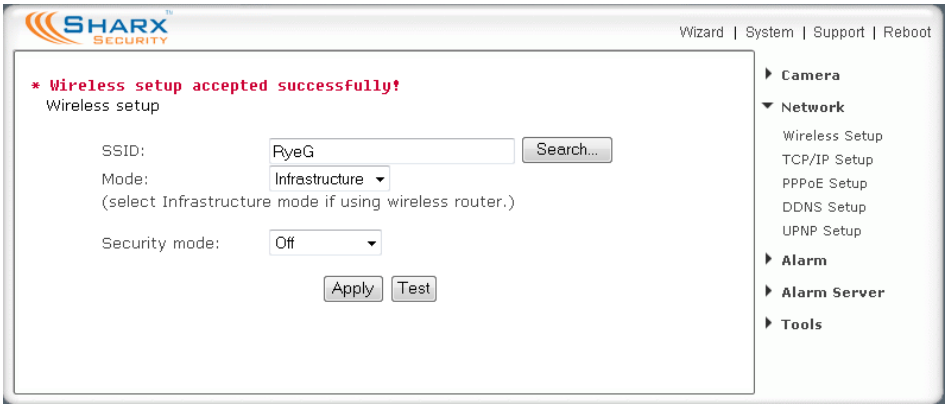
Click on "Network", then click on "Wireless", and you'll get to this screen:



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:



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.

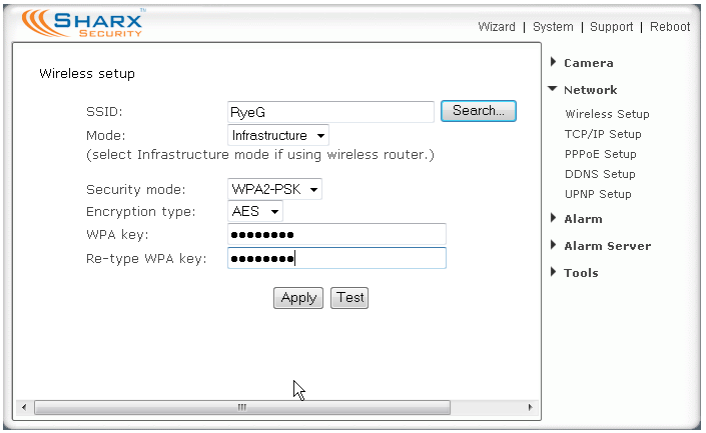


Please make sure “Infrastructure” is selected before proceeding, since that is the most common type of network. “AdHoc” is for network experts only.

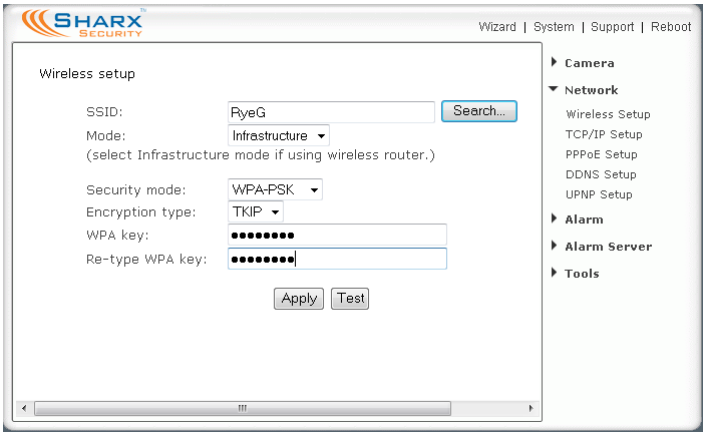
The “Security mode” needs to match the type of wireless password used on your router exactly. The old type is WEP. Newer routers may use WPA or WPA2 passwords (keys).

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:



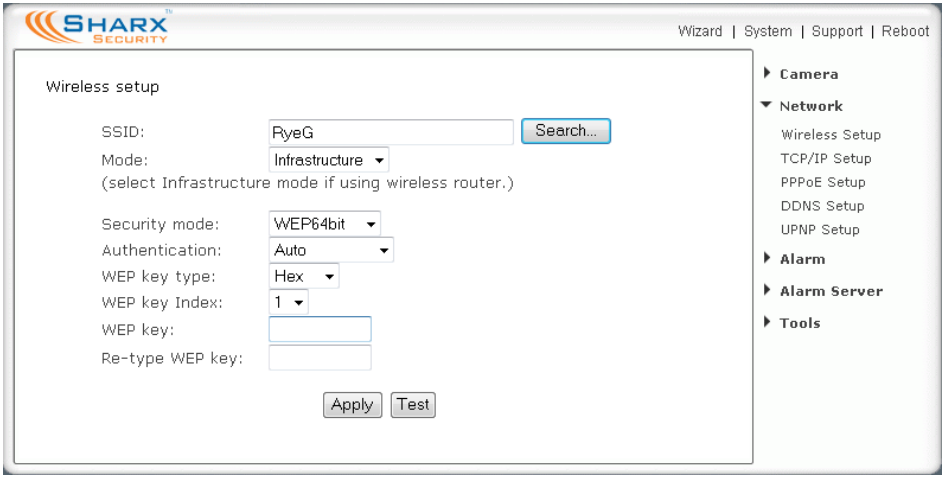
However, older Apple Airport and many other routers use WPA with TKIP:



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 ` ” ‘. 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 information was stored in the camera. Now you should use the “Test” feature to check if you typed it correctly.

If the test reports “Success!” 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 “Success!” 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, do not forget to 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 computers. The MAC address is printed on the back of the camera.

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 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, and concrete with metal rebar can be a 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.

If the Wifi channel is set to "Auto", we recommend changing it to one of the following fixed Wifi channels: 1, 6 or 11.

On N mode 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 130/150 mb speed**". Mixed 20/40 Mhz should be avoided.

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.

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 all 4 possible combinations. On a laptop you typically do not need to specify the exact password type since the laptop will try everything automatically. The camera is more picky, it needs to know exactly what type of password you are using and 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. However, as long as the cable is still attached, the camera's "**System**" menu will show "**No wireless connection**".

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. This is called "port forwarding" and is done with Airport Utility 5.6 as follows:

In the Airport utility, go to manual setup and select the gear-shaped "**Advanced**" icon. Click on "**Port Mapping**", then click on the **+ (add)** icon at the bottom of the box, and enter the following info:

Service: (don't change this, leave at "Choose a service" or "Custom…")
Public TCP port: 8150 (your 2nd camera would have 8151 here, 3rd 8152 etc)
IP address: (add the IP address for your camera, e.g. 10.0.1.4)
Private TCP port: 80

Leave other entries blank, then "**Continue**", and add a description like "SharxCam1HTTP", then "**Done**", and click on the **+ (add)** icon again. This time use the following settings:

Service: (again don't change)
Public UDP port: 30000-30001 (next camera would have 30002-30003 etc)
IP Address: (again the IP address for your camera)
Private UDP port: 30000-30001 (same as public UDP port)

Leave all other entries blank, then "**Continue**", and add a description like "SharxCam1RTP", then click on "**Done**" and "**Update**" to restart your Airport.

Now someone from outside your network should be able to access your camera using your external IP address with **:8150** added to the end. For example, if the Airport summary screen shows your IP address as 12.34.56.78, you would enter the following in your browser: http://12.34.56.78:8150

This assumes your Airport is your only router. You can check this by going to www.checkip.org. The IP address shown there should be the same as shown in your Airport. Otherwise you have multiple routers and networks. In that case you would need to forward ports through the preceding routers with DMZ or "Static NAT". Or you could set your other routers to "bridge mode" to avoid complications of multiple sets of local IP addresses.

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 similar, 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.

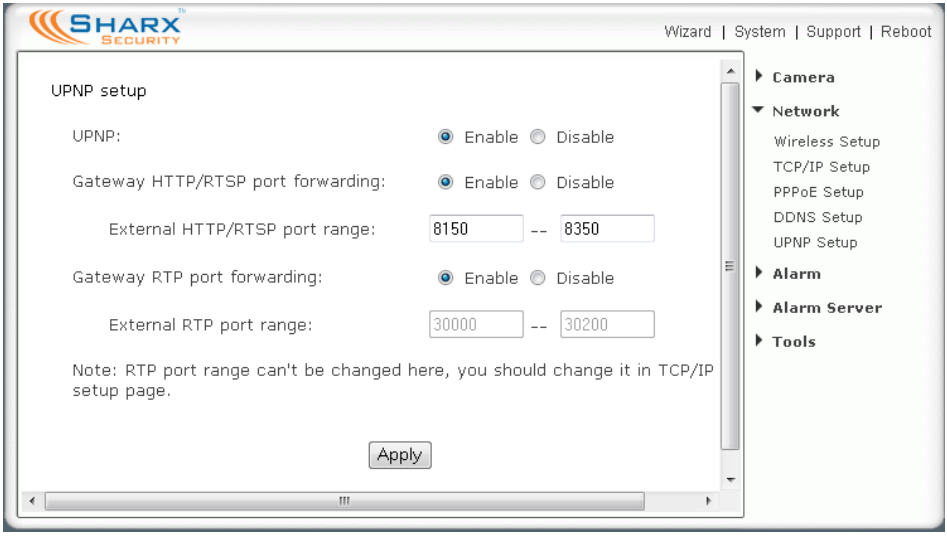
Enabling UPnP for Automatic Remote Access Setup

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

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, or DLink model as they are very inexpensive now (we've seen sale prices under $40). Either way our tech support can help you.

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 last 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.

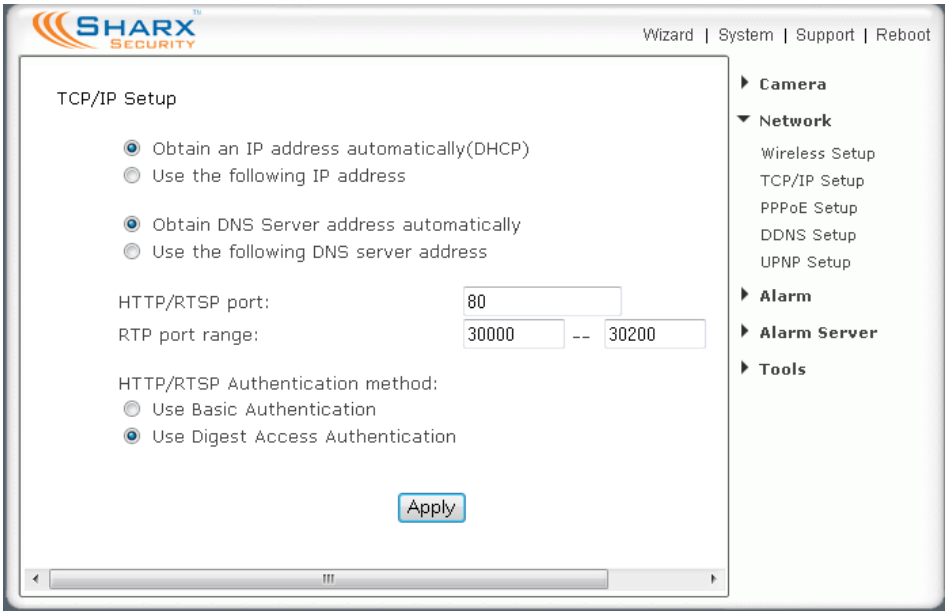
The router uses addresses in a range set aside for this purpose (called the DHCP range). For many routers, this DHCP range is from 2 to 100 but you'll have to check your specific router's DHCP menu. Sometimes this is shown as start and end address, or start address plus number of available addresses.

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 192.168.1.2 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 255 since that is the highest possible limit.

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":



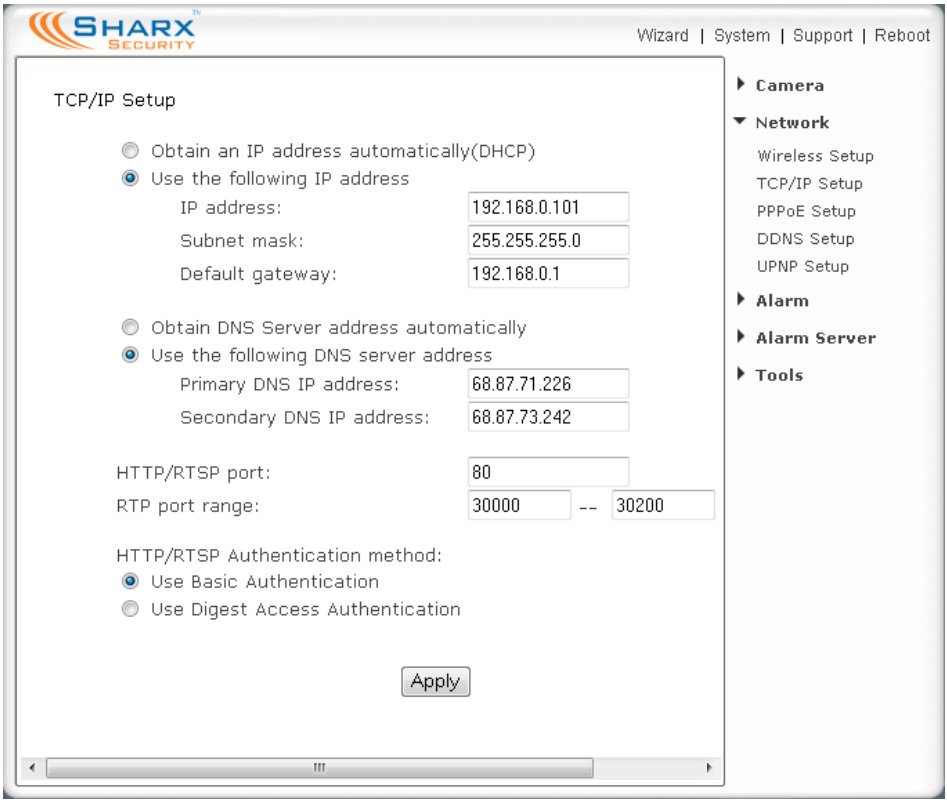
Click on "use the following IP address". Then enter the IP address you picked that is outside your router's DHCP range. Do not change the subnet mask. The default setting of 255.255.255.0 is correct unless you have a very unusual home network.

Then enter your own router's address in the "Default Gateway" box and also in "Primary DNS IP address". **IMPORTANT: Do not leave these fields blank!**

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.

Note: 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



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.

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 the port, too.

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" for the camera. This basically means that any request from the internet is forwarded to your single camera. However many of our customers use more than one camera so we will explain the port forwarding procedure.

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 and www.dyndns.com are the recommended companies for "Dynamic DNS" service. Also known as DDNS, this is a totally free service that allows your own name to be assigned to your camera. This name takes the place of the 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 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 create a free account with one or both of these companies. We'll take www.no-ip.com as an example. The "create account" function is on the top right under the Username/Password fields. Do not register a domain or sign up for any other paid services. You just need the free account.

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" 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 in their case there is an additional step of checking out a shopping cart with a zero dollar fee.

Now proceed to the next section to make sure your name is updated correctly.

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 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 SCNC2607 and other models with IR night vision have several settings to adjust your preferred night vision.

The IR infrared LEDs can be set to “On”, “Off”, or “Automatic” which uses the 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 this setting “Off”. It’s worth a try.

The “Moonlight mode” setting in the “Camera Setup” menu boosts available light by reducing the frame rate to 7.5 fps. On the SCNC2606 this feature can only be set “On” or “Off”, while other models have the additional “Automatic” setting. This uses the light sensor to turn on moonlight mode only at night.

If you are using indoor IR cameras to look through a window, you should set IR LEDs to Off and instead set the Moonlight mode to Automatic. Otherwise the IR LEDs would reflect off the window glass and the glare would make everything almost invisible.

The outdoor cameras and the new SCNC2700 series have a feature that combines the excellent daytime colors of the SCNC2606 with the IR night vision performance of the SCNC2607. During the day, an optical “IR cut filter” removes all infrared light. This makes the camera’s daytime vision similar to a human eye which does not see IR light, and therefore all colors appear vivid and natural to us. 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 & night.

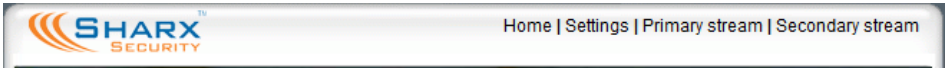
If using the SCNC2700 to look through a window, you may want to experiment with the IR filter in the automatic position even though IR LEDs are set off. Combined with automatic moonlight this makes the best use of street lighting.

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, Firefox, or Chrome Browser

When using a Mac with Safari or Firefox to view the camera, or when using a PC with any browser other than Internet Explorer, the browser's standard method of displaying video is MJPEG (Motion JPEG) without audio.

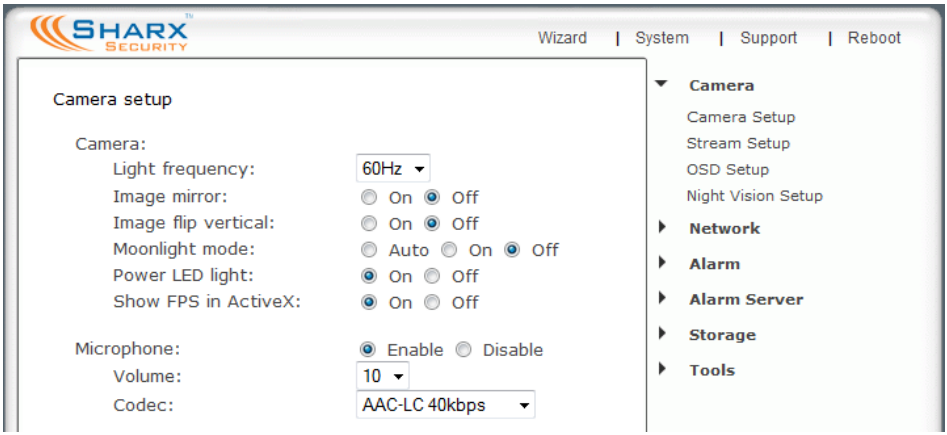
It is easy to switch to MPEG4 video with audio. Just make sure that Apple QuickTime Player 7 is installed on your Mac or PC, then while viewing the camera's video in Safari click on "**Primary Stream**" or "**Secondary Stream**" at the top of the browser screen. (Secondary stream has a smaller video window)



This will start the QuickTime Player plugin inside the browser. After logging into QuickTime you will see even better quality video than the browser can display, and the video will have high quality audio as well.

If you have a smaller computer screen or many open windows and the video appears paused, it is likely that the QuickTime login window ended up behind the browser. In that case you just need to move the browser window a little bit to see the QuickTime login window underneath. QuickTime might ask twice for login info. You can reduce that by saving your username/password so that it is already stored in your computer. In that case, be sure to update or delete stored passwords on your computer if you ever decide to change the camera's login info. Otherwise QuickTime would get stuck at this step.

For audio on Mac OSX Lion, the camera needs to be in its default configuration with the AAC audio codec selected in the "Camera Setup" menu:



Positioning and Mounting

The VIPcella series cameras have standard tripod mounts and are compatible with regular photo tripods or security camera mounts. If you want to use a tripod we recommend the very inexpensive QuantaRay / SunPak QSX2001, which is available for under $25 from photo supply stores.

Indoor cameras: The included desktop stand can also be used for wall or ceiling mounting. For some angles you may need to loosen the main mounting ring by turning the big flat screw on the back of the bracket with a coin, so that the notch in the mounting ring allows the pin to point in the desired direction. You can then tighten it again with the coin. Should any mounting position require the image to be rotated 180 degrees (inverted), there is a setting for that in the "camera setup" menu.

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

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.**

In a typical scenario the camera is mounted to a wall with the supplied adjustable mounting bracket. The bracket is usually attached to one of the 3 mounting points at the bottom of the camera. Additional mounting points are usually covered with a removable white rubber plug. Do not try to remove the silver colored disk at the bottom of the camera, that's the microphone and any attempt to remove it will destroy the microphone's internal connection.

The easiest way to mount the outdoor camera to the wall is to mount the bracket first, as in this sequence:

1) Completely loosen the ball joint of the mounting bracket with the supplied Allen wrench

2) Detach the silver mounting rod from the bracket base, and secure just the bracket base to the wall by itself

3) Screw the silver mounting rod into the camera, first hand tighten it, then lock it with the white plastic lock wheel

4) While holding the camera with one hand, re-attach the ball joint, aim the camera direction, and tighten ball joint. This way, you never need to turn the camera in a direction that would loosen the mounting rod

Alternatively you can replace one of the camera's sunshield mounting screws with the special 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.

For outdoor cameras 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 completely erase/reformat the MicroSD in a computer with an SD card slot.

Based on feedback we received from customers, the cable connection now terminates into a breakout box for a neater installation. You can mount the breakout box to the interior side of a building's wall if you feed the wire through a ¾" hole in the wall. Or you can keep the breakout box outdoors, using the weatherproof metal shell that encloses the breakout box. In that case you would keep the weatherproof silicon gasket on all connections that you are not using. We also included a metal bracket that can be used for secure attachment of the breakout box to a wall.

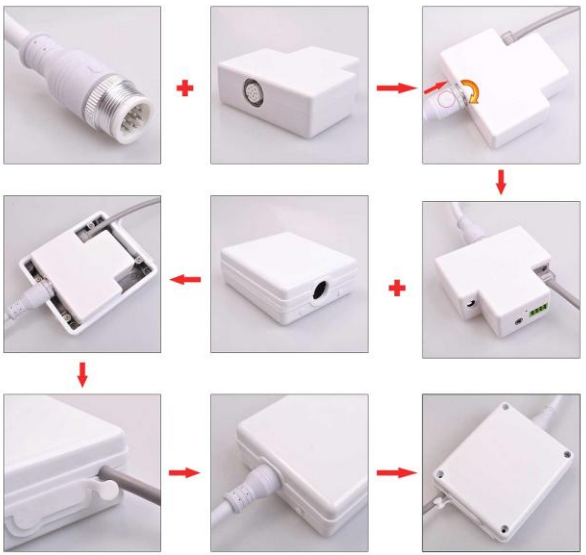
Please note that this AC adapter cannot be exposed to moisture. If you use the AC adapter outdoors, it would have to go into an outdoor power outlet with a completely enclosing cover. For example, see “Code Keeper” or similar brands.

If you need more than the length of the power cable on the AC adapter, you can extend it up to 50 ft using splice connectors and any low voltage wire such as doorbell wire or telephone wire. Home Depot sells this type of wire for about $0.10 /ft. The solderless, waterproof splice connectors are about $5 for a pack of 25. **IMPORTANT: Do not swap plus and minus or the camera will be damaged beyond repair. This type of damage is not covered by warranty.**

Please note that after initial setup only the power cable is required for the wireless model SCNC3605. The wired/PoE model SCNC3606 can be either connected with power cable and Cat5, or optionally just with a Cat5 cable that is connected to an 802.3af PoE compatible switch. We recommend a NetGear FS108P or GS108PE PoE switch, or the single port Dlink DWL-P200. All remaining connections are entirely optional and described in the Appendix.

Below is an illustration showing how the cable from the camera is attached to the breakout box, and how the breakout box can be mounted in the included weatherproof shell if it is desired to mount the breakout box outdoors.

Do not forget to attach the mounting bracket to the shell and to use the rubber plugs to cover the screw holes for the neatest installation.



Motion Detection or Timed Emails and FTP Uploads

The camera refers to motion detection as an “alarm”. You can select what you want the camera to do once the motion is detected.

One option is to set up the details of your email server account and have the camera send you JPEG snapshots. These picture files are compatible not just with computer based email clients, but now also directly compatible with Apple iPhones and other web-enabled cell phones.

So your camera can alert you on your cell phone with a picture or series of pictures 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 your FTP server (or a NAS hard drive with built-in FTP server)

One thing to keep in mind when sending pictures to cell phones is that without an unlimited data plan you may 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. So be careful and test it on a computer with free email first.

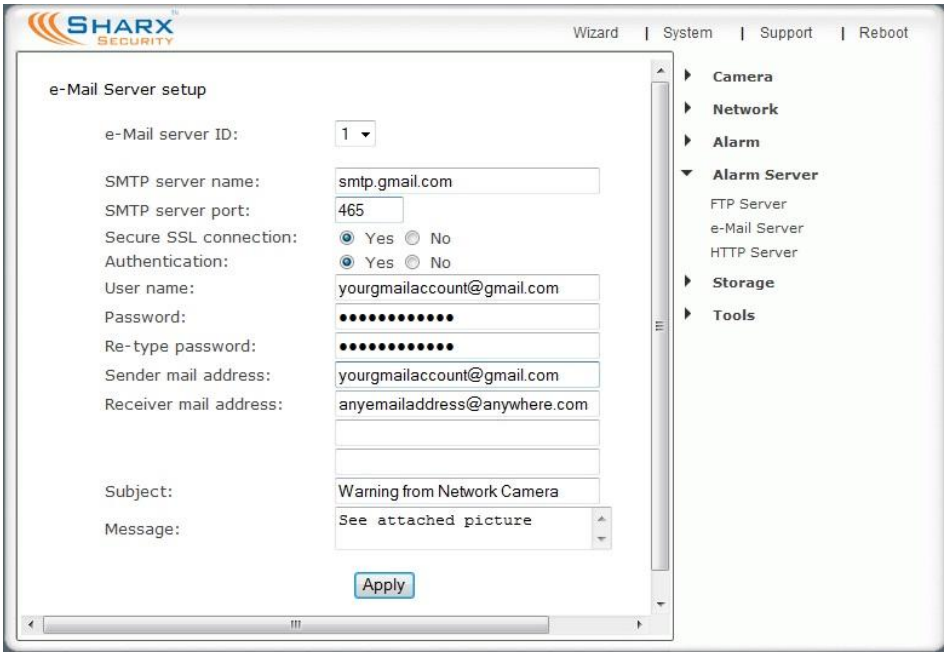
The factory default setting for motion detection is a single motion detection window covering the entire visible area. The “Motion Detection” menu allows you to designate up to 4 separate windows with individually adjustable sensitivity, however you should keep this menu at default settings until you 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 “Alarm Server” and “Alarm Management” menus.

For automatic emailing you will need both an outgoing email server and one or more email receiving addresses. If you don’t have this information handy you may want to refer to your internet service provider’s help pages or your Microsoft Outlook or other email program account settings.

Following is an example of a proper configuration for using Gmail as the outbound server, which then can send email to any receiving email address.



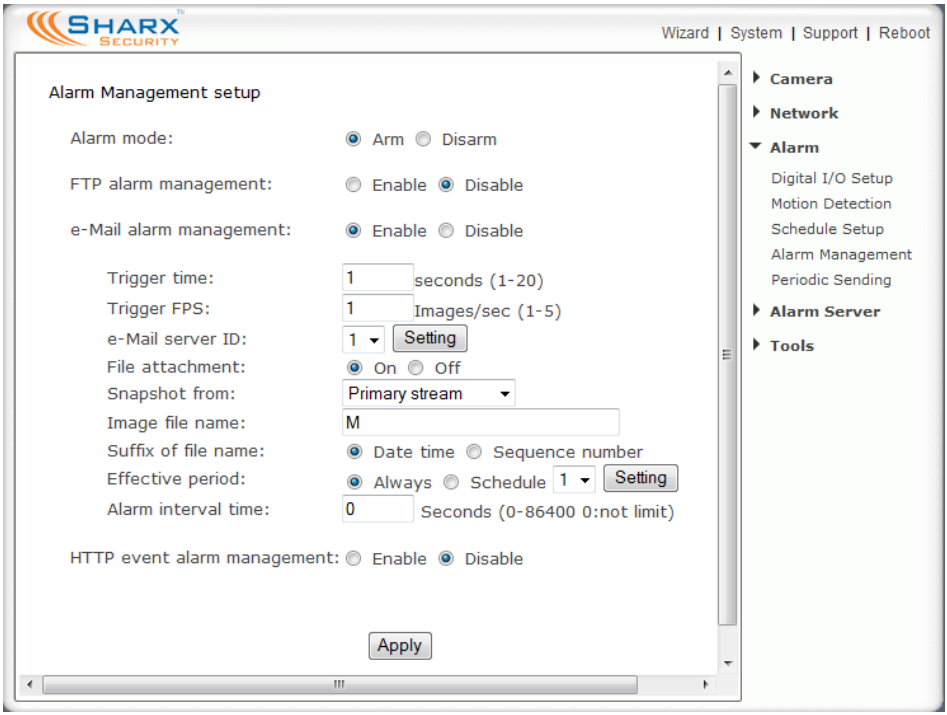
Note: **Gmail requires that you go to your account settings on Gmail.com and enable POP, disable IMAP, and with a browser other than Google Chrome, select "Basic Attachments" in the "General" settings tab. Chrome hides this option. Important: Without these Gmail settings the camera can't send email**

Note that if you have a typo in any of this 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**
- 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 sending email. You can also send email to several receiving email addresses, 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 an @ symbol.

After setting up the email server you would then enable the email alarms through the alarm management menu. Common settings are shown below:



Trigger time and trigger FPS (frames per second) have the following meaning:

When motion detection is triggered, send pictures at the rate of “Trigger FPS” frames per second for the duration of “Trigger time”. Here is an example:

If trigger time had a value of 4 and trigger FPS had a value of 2, you would be getting 2 images each second for 4 seconds in a row, meaning 8 pictures total for each motion detection event.

If you do not want pictures, you can turn “File Attachment” off. For smaller pictures you can select from “Secondary Stream” or “Mobile Stream”.

It is useful to have a short prefix for the file names, such as M for motion. The rest of the generated file name can include time & date or a number.

The “Alarm Interval time” allows you to designate a time (in seconds) during which new emails are suppressed. For example, to avoid a flood of emails and risk having your email account blocked for suspected spamming, you should set this time to 600 seconds to prevent additional emails for 10 minutes.

If you prefer, you can have the pictures uploaded to an FTP or HTTP server instead of an email address. There are many choices for FTP servers.

For example, you could enable the built in FTP server function on one of your computers or download free FTP server software such as FileZilla.

Another possibility is to use an online (cloud) account with FTP access, such as DriveHQ.com which is available for free with a limited amount of storage.

Yet another option for FTP server is to use a standalone NAS (Network Attached Storage) hard drive such as NetGear ReadyNAS.

Setup of the FTP server menu and the FTP alarm management menu is very similar to setting up the email server and email alarm management.

FTP Server: At a minimum you need the IP address and login info for your FTP server. The port is almost always 21, and typical servers need a username and password which means “Anonymous” should be set to “No”. The setting of “passive mode” and Keep Alive is dependent on your server. If you don’t know what to put there, try both settings for passive mode and 3600 seconds (one hour) for Keep Alive.

FTP Alarm Management: Most settings are almost identical to the email alarm management. You do not need to specify a remote path unless you want to keep the files organized into folders. In that case you’d need to make sure the spelling of your path is identical to the name of your folder on the server.

If you maintain your own web page there is a neat feature available by setting the file suffix 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.

The following chapters will show even more possibilities to use motion detection. For example, you can use motion detection to initiate the recording of video or snapshots to MicroSD card. Or you can use motion detection together with our MultiLive PC software to record video while economizing on storage space by recording only when there is motion.

Instead of using motion detection you can also use the **“Periodic Sending”** menu to email or upload pictures at regular time intervals.

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

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 (NAS) drive
3) One-click recording on a Windows PC using Internet Explorer
4) Recording on a PC with the included MultiLive software or commercial software (BlueIris, LuxRiot)
5) Recording on a Mac with software such as EvoCam 3.75 or 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.

Recording with a computer would require the computer to remain on at all times without being allowed to go to sleep or standby, but does have the advantage that the highest frame rate settings can be used.

For the MicroSD or NAS recording method described above, or for recording multiple cameras, or for recording in combination with any other features such as live viewing, email or FTP, you should reduce the settings in the **"Stream Setup"** menu as shown below:

Primary Stream: Image size: 640x480, Frame rate: 15, MPEG4 bit rate: 1024K, MJPEG quality 50, Snapshot quality 90

Secondary Stream: Resolution: 320x240, Frame rate 15, MPEG4 bit rate: 256K, MJPEG quality 50, Snapshot quality 90

The following settings should remain at the factory defaults:

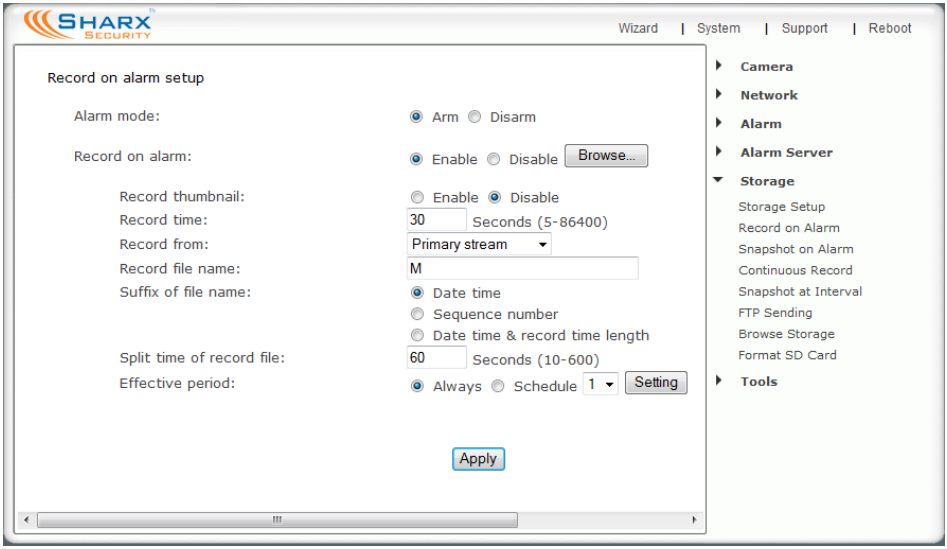
Mobile Stream: Resolution: 176x144, Frame rate 5, MPEG4 bit rate: 20K, Snapshot quality 70, RTSP authentication: alternate

The **"Camera Setup"** menu should have the microphone audio codec setting of AAC-LC 32kbp, 24kbps, or 16kbps. Selecting AMR can cause both audio and video skipping and stuttering, so we recommend recording with AAC only.

Recording to built-in Micro-SD card

All new V*IPcella* series cameras can now accept MicroSD cards up to 16 GB. All cards should be fully formatted prior to use with the official software from http://www.sdcard.org/downloads. A pre-formatted card is included with outdoor cameras only. The card slot is at the bottom or side of indoor cameras and behind the lens cover of outdoor cameras. (See diagram on next page)

When the camera powers up with a MicroSD present in the slot, the "**Storage**" menu allows you to format the MicroSD, browse the contents, or set up continuous or motion detection (alarm) recording of video clips in Apple QuickTime MOV movie format or snapshot pictures in JPEG format.

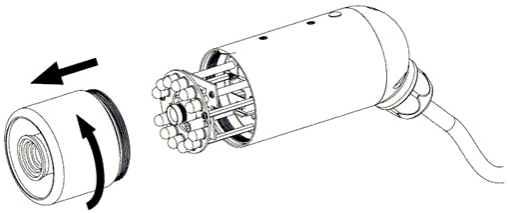


The resulting video files can be viewed with the free QuickTime for Windows or Mac. Please note: Windows Media Player can also play the movie files but cannot play the sound. If your PC automatically plays movie files in Windows Media Player you can uninstall and reinstall QuickTime Player to fix this. Shorter video clips will download much faster. If you have many video files you could also remove the MicroSD card and access it directly from your computer (with suitable adapter if needed). This is only practical for indoor cameras due to easy accessibility of the MicroSD card slot.

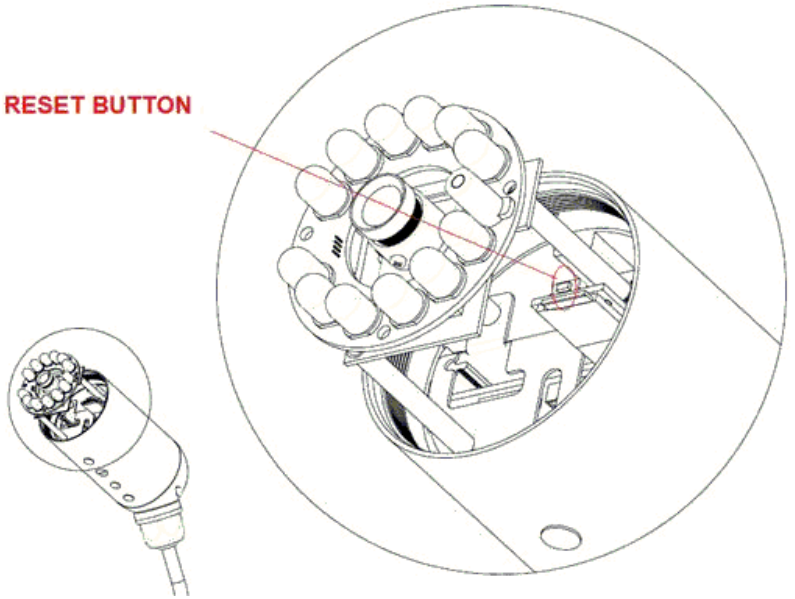
Please do not remove the MicroSD card while recording is active. If you have recording enabled, you should disable recording and wait 1 minute before removing the card.

Errors caused by removal during recording might require reformatting.

To access the MicroSD card slot on the SCNC3605/06, please bring the camera indoors (in an area of 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 MicroSD card slot is right under the reset button shown below:



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.

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.

Using the camera as a continuously recording DVR

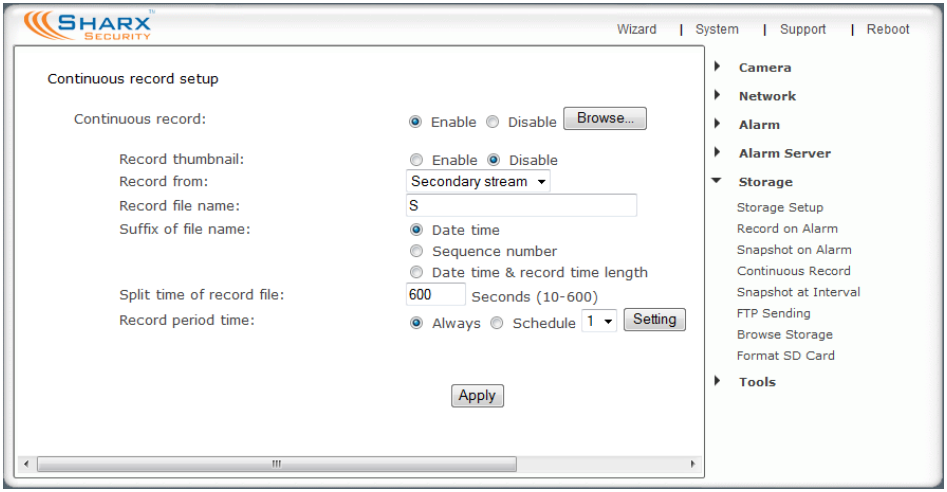
With the larger MicroSD cards it is practical to use the camera as a continuously recording DVR (Digital Video Recorder) with the right settings.

A 2 GB MicroSD card has about 1872 usable megabytes of storage space after formatting. At the very highest settings of video quality with highest picture size, this is only about 2 hours worth of storage.

However, if you set up the "Secondary Stream" in the camera's "**Stream Setup**" menu with 320x240 resolution, a frame rate of 10 fps, and bit rate of 120K, this will be reduced to about 12 megabytes per 10 minute clip or 75 megabytes per hour, which allows 24 hours recording time on the 2 GB card.

With the maximum supported MicroSD size of 16 GB card this can be extended to slightly over 1 week, or you can instead increase video quality.

Increased MPEG4 bit rate improves image sharpness while increased frame rate makes motion appear smoother. The camera supports a frame rate of up to 15 fps and a bit rate of up to 1024K for recording to MicroSD or NAS drive.



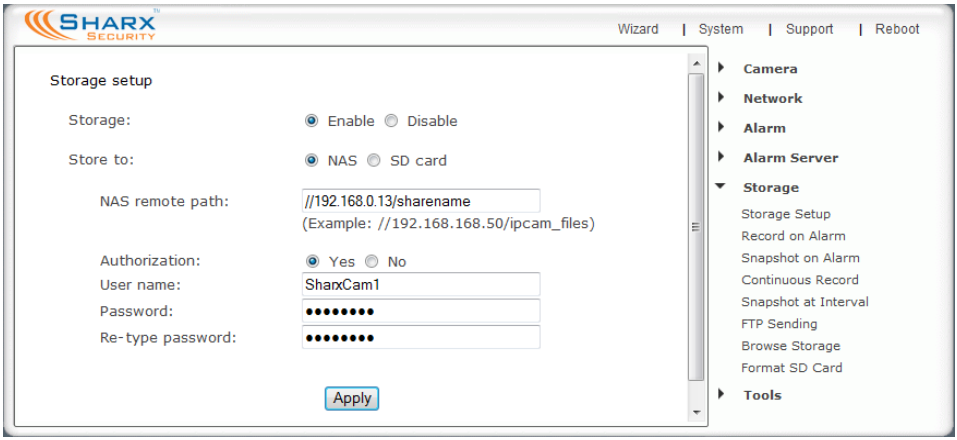
To limit file sizes, video is recorded in clips of up to 10 minutes (600 seconds). You can then view your files in the "**Browse Storage**" menu in the "**Continuous Record**" folder. There will be 6 files per hour in QuickTime MOV format. After the MicroSD card is full or the limit of 1000 files is 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 the IP address of the drive and the "**share**" name. You need to make sure your NAS drive has a permanently assigned IP address that does not change after a restart.

Tested NAS drives include the **MyBook World, NetGear ReadyNAS**, and **Apple Time Capsule** when set up for "SMB file sharing" with accounts.

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

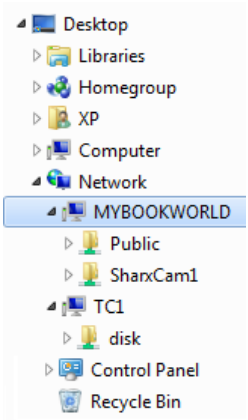


The share name is the name of the top level folder that a NAS drive shows on the network. You can check it by clicking on the icon for the NAS in your PC's "Network" or "My Network Places" folder, or on a Mac by using Finder, then "Go to…" and "Network" and then clicking on the NAS icon.

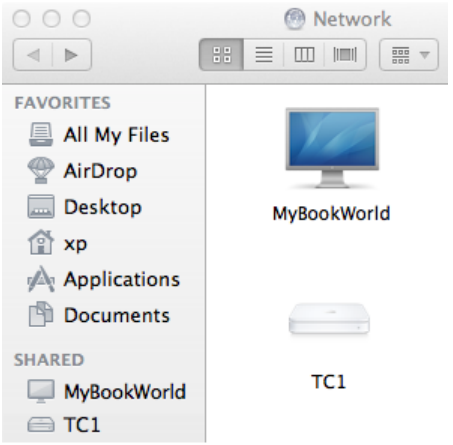
In the example on the next page, the drive TC1 has a network share named "disk", and MYBOOKWORLD has the shares "SharxCam1" and "Public". For NAS drives **other** than Apple Time Capsule, **if your share name has spaces in it you need to rename it without spaces**. Each NAS drive has its own menus, consult 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:

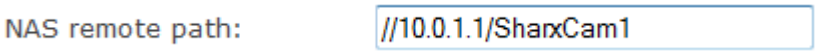


Network folder as shown on a Mac:



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:

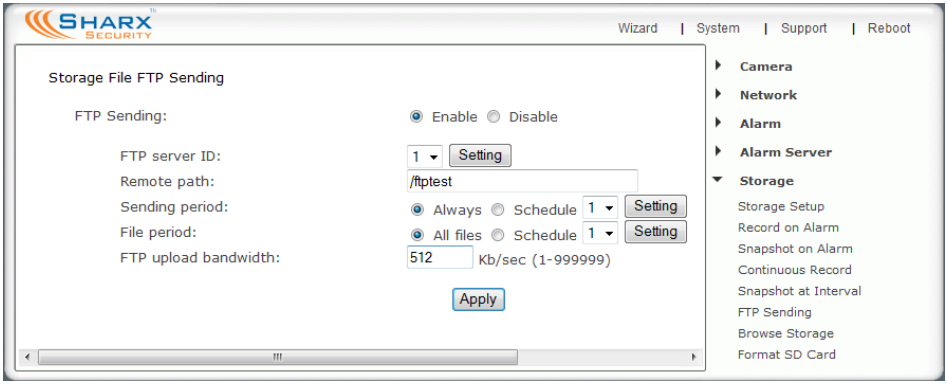


Then click on "Yes" for authorization, enter the username and password for the account you created, "Apply", and after about a minute click on "System" at the top of the camera's settings screen again, and scroll all the way down to the storage section. You should have a NAS status of "Ready" and lots 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 limit of 10,000 files is reached or storage is full, the oldest files are deleted.

Automatic Uploading to 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 “FTP sending” menu. Unlike NAS, FTP works over the internet.



First you would set up your FTP server account information in the camera’s “Alarm Server” menu as described in the chapter about motion detection.

“FTP upload bandwidth” is an optional setting to slow down FTP transfers if you do not want a slow internet connection to be overwhelmed. For locally connected FTP servers we recommend a value of 2000 or higher, for remote servers we recommend 512 or half your available internet upload speed.

“Remote Path” specifies the folder on the FTP server. Some FTP servers require this to be blank, others require the exact name of your existing folder (and you need read/write/delete privileges for that specific folder).

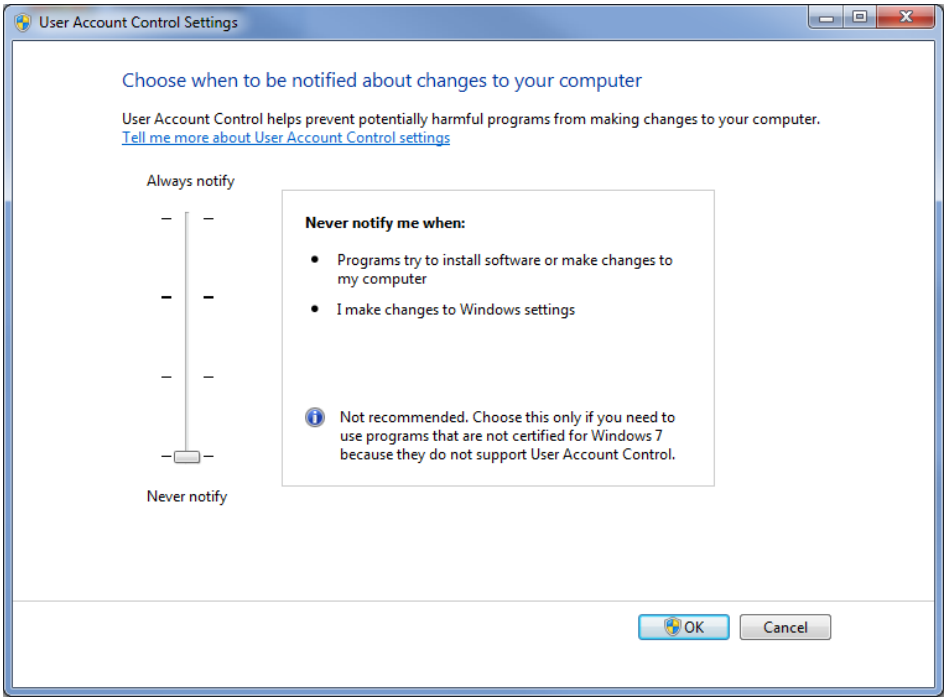
Once successfully transferred, each original file on the MicroSD card is deleted. To prevent files from piling up on the MicroSD card, the rate at which the files can be transferred to your FTP server has to be much faster than the rate at which new files are created, and therefore this feature is generally 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 features you really need.

Recording Video using a Computer

If you prefer to record video using a computer, there are several different options. On PCs with Internet Explorer the simplest method is to just press the red record button while viewing your camera. Be sure to use the button with the wrench icon first to select a proper folder for storage of your recorded video, and for motion detection recording select the “alarm” checkbox.

For Windows 7 and Vista users: Recording will only work if UAC (User Account Control) is turned off. In the Vista Control Panel, choose “Security”, then “Check this Computer’s Security Status”, then turn off the User Account Control at the bottom. Windows 7 has this setting in “User Account Control”



For recording multiple cameras, or for more recording options such as limiting the amount of space or circular recording, you can install the MultiLive software that we are also providing on the CD

MultiLive is only provided for PCs with XP, Vista, or Win7. Mac users can use the camera’s built in MicroSD recording or commercially available software. We recommend EvoCam 3.75 from www.evological.com and SecuritySpy from www.bensoftware.com. Some software packages have free demos to try.

MultiLive: PC Software for Multiple Camera Recording

Once installed, the included PC MultiLive software allows you to view and record multiple Sharx IP cameras at the same time.

The menus are fairly straightforward. You add cameras with the Camera Manager menu (under Option) then you activate them with the Connect menu (under Control). Recording starts when you click on the Record button (on bottom right) or use the Record menu. If you only want to record motion then you use the Alarm menu (or Bell icon) instead of Record.

To make sure you are not overwhelming your local network or your internet upload bandwidth, be sure to use the stream setup described on page 40. MultiLive always uses the Primary Stream settings. To accommodate more than 4 cameras you should reduce the primary stream image size to 320x240, frame rate to 15 fps or less, and MPEG4 bit rate of 256K or lower. Or you could use a commercially available software package such as BlueIris from www.blueirissoftware.com or LuxRiot from www.luxriot.com. These software packages allow recording from the secondary stream while you have your primary stream settings optimized for viewing the camera, in addition to many other professional features such as automatic restart after power failure.

Viewing Live Video on your Cell Phone

As with using a computer, you connect to the camera with your cell phone by typing the complete IP address into your browser or by selecting from previously entered bookmarks.

If you're connected via Wifi to the same local network as the camera, you would use the local IP address (usually starts with 192.168 or 10.0)

If connected remotely, you would first make sure you've completed the "remote access setup" as described in earlier chapters and then you'd use your camera's external IP address and port.

With an iPhone you would use Safari to connect to your camera exactly the same way as you would with a computer. Also please see the next chapter for our experience with various commercially available iPhone / Android apps.

With other cell phones such as Droid, Blackberry, and Windows Mobile etc, you would use your camera's IP address and then add **/mobile** at the end. Don't forget the port number. For example, one of our demo cameras is at

http://sharxdemo2.servehttp.com:8150/mobile

If your cell phone shows the 3 buttons on the initial screen so small that the lettering is hard to read, either zoom in or just remember that the top button is for pictures and the middle button is for live video. The third button is for fine tuning settings but if the writing is too small to read you may want to change settings only from your computer and not your cell phone.

If the picture works but video doesn't, try different "RTSP authentication" settings for the Mobile Stream in the camera "Stream Setup" page. The RTSP authentication OFF setting removes password protection and is not advised.

On some cell phones (e.g. SonyEricsson) the first time you click on the 3GPP stream button it may fail but it will work if you try it again.

If your cell phone has a setting for Java or Javascript it needs to be enabled.

Still, passwords can cause problems. In that case we recommend to go to the first button (Picture live) and then entering your username and password with the "Save Password" option on your cell phone checked.

If you want to save time or you want to explore other options, there are ways to get to the different video streams without the initial login screens. The "Camera Setup" page in the camera has the details of all the available streams.

If you click on the blue underlined words "Mobile Stream" you'll get the list of video streams that are most suitable for cellphone access. For example, if your camera is at http://sharxdemo2.servehttp.com:8150 then you can access the mobile video stream directly with the following URL:

rtsp://sharxdemo.servehttp.com:8150/live_3gpp.sdp

On some cell phones this RTSP stream cannot be opened by the browser and instead needs to be opened by the media player with the "Open URL.." menu. In that case the RTSP authentication setting should be "Enable for Quicktime"

In case of problems you may want to initially select the lowest bandwidth video by going the camera's Mobile Stream Preset and selecting "GPRS low bandwidth". For troubleshooting with a computer, set RTSP authentication for the mobile stream to the off or PC setting, then open the 3GPP mobile video stream using the "Open URL…" menu in Apple's QuickTime Player 7 or the VLC version 1.xx media player from www.videolan.org

On Android based cell phones we recommend the tinyCam app shown in the next chapter.

The one stream type that is supported by virtually all browsers is the single JPEG snapshot. Just use your camera's external IP address, add /snapshot.jpg and you can see a current big picture. For example:

http://sharxdemo2.servehttp.com:8150/snapshot.jpg

Note that streaming video on the cell phone requires the UDP ports to be set up correctly. This is done automatically if you have the UPnP feature on your router. For manual setup, refer to the port forwarding section of this User Guide. The default setting is to have UDP ports 30000-30001 to be forwarded to the camera. You can test this by using QuickTime or VLC as described above. If QuickTime from a remote computer can play the mobile stream then all the port forwarding is correct. After testing with QuickTime, you'll probably need to set the RTSP authentication for the mobile stream back to "Alternate".

iPhone Apps

All Sharx VIPcella series cameras can be viewed without any changes using Safari which is available on all iPhone, iPad, iPod Touch devices. However, Safari does not have built in support for MPEG4 video with sound. Below are some other iPhone/iPad apps we tested recently (as of March 2012):

IPVision ($10). Compared with Safari this app allows a borderless landscape view to take full advantage of the entire iPhone screen. Also allows quick, one-touch cycling through many cameras. We have customers with 12 or more cameras using this app to access all their cameras. Currently no sound support.

EyeCam ($4.99) Also good for viewing many cameras. Easy setup, no sound.

Baby Monitor HD ($9.99). This app supports sound on iPhone and iPad if the sound selection in the Sharx camera's "Camera Setup" menu is set up with AMR 5.9k. Please note that Mac OSX Lion requires the AAC sound setting, so switching between a Mac and Baby Monitor HD would require changing the audio setting in the camera's "Camera Setup" menu. In the camera's "Stream Setup menu, we recommend using frame rate: 15 fps, MPEG4 bit rate 1024K.

Android Apps

One recommended app for viewing our cameras on Android is **tinyCam**
On an Amazon **Kindle Fire** tinyCam can show 4 cameras at the same time.

For setup, be sure to select "Sharx Security" in the camera vendor field.

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: 192.168.0.46

For local cameras the default value for the port field is usually correct: 80

For a remote camera you would add just the hostname or IP address in that field, for example: sharxdemo2.servehttp.com

For the first remote camera the value for the port field 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.

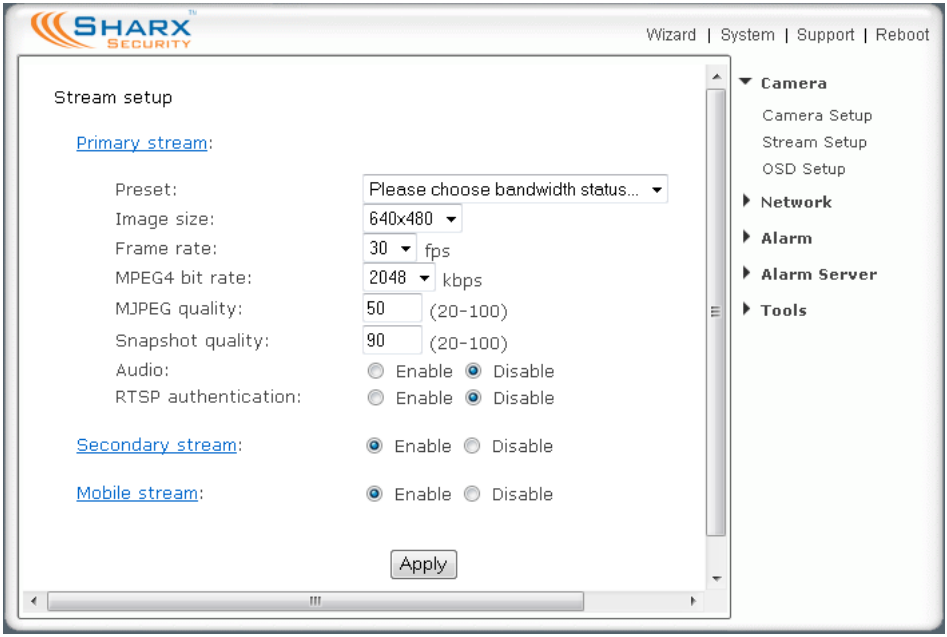
As of March 2012, tinyCam is working to add audio support for Sharx cameras.

Audio/Video Stream Reference

The Sharx VIPcella series of cameras is very versatile and supports multiple simultaneous video streams. Entering through the main login screen automatically activates the highest resolution video stream, called the Primary Stream. On a PC with Internet Explorer this will be MPEG4 video with audio.

Other browsers like Safari and Firefox cannot automatically install the ActiveX MPEG4 decoding and recording software and in that case the Motion JPEG stream will be automatically selected. While MJPEG does not support audio, Macintosh users can play MPEG4 with audio and video through QuickTime as explained below, or by using the new “Primary Stream” and “Secondary Stream” shortcuts at the top of the main video screen (see page 32)

For access to specific types of audio or video encoding, you can bypass the main login screen and go directly to a link for the camera with the desired protocol and encoding type. The full list is accessible by clicking on the blue underlined “Primary Stream”, “Secondary Stream”, or “Mobile Stream” links in the Stream Setup page.



On a network with UPnP, clicking on “Primary Stream” will result in this list:

Primary stream list

Intranet stream URL	
RTSP MPEG4 stream:	rtsp://192.168.0.21/live_mpeg4.sdp
RTSP MJPEG stream:	rtsp://192.168.0.21/live_mjpeg.sdp
HTTP MPEG4 stream:	http://192.168.0.21/stream.av
HTTP MJPEG stream:	http://192.168.0.21/stream.jpg
HTTP ASF stream:	http://192.168.0.21/stream.asf
HTTP snapshot image:	http://192.168.0.21/snapshot.jpg
Internet stream URL	
RTSP MPEG4 stream:	rtsp://sharxdemo.servehttp.com:8150/live_mpeg4.sdp
RTSP MJPEG stream:	rtsp://sharxdemo.servehttp.com:8150/live_mjpeg.sdp
HTTP MPEG4 stream:	http://sharxdemo.servehttp.com:8150/stream.av
HTTP MJPEG stream:	http://sharxdemo.servehttp.com:8150/stream.jpg
HTTP ASF stream:	http://sharxdemo.servehttp.com:8150/stream.asf
HTTP snapshot image:	http://sharxdemo.servehttp.com:8150/snapshot.jpg

You will notice that some entries start with “RTSP:” instead of “HTTP:”. This is not a typo. **RTSP streams can be opened by the “Open URL…” menu in Apple QuickTime 7 on Windows or Macintosh with audio and video**. Linux enthusiasts may want to try the VideoLAN VLC Media Player, version 1.xx

NOTE: QuickTime 7 works very well. The new QuickTime X in Apple’s OSX Snow Leopard or Lion has problems with passwords. QuickTime 7 is available from Apple.com for OSX Snow Leopard, OSX Lion, and also for Windows PC. Quicktime X on Lion also requires the camera audio to be set to AAC codec.

A quick summary of the different available formats:

MPEG4 is true full motion video with audio. Internet browsers typically cannot show this without an add-on program. On PCs with IE7 - 10 the required add-on program (also known as ActiveX) is installed and activated automatically if you click “Enter” on the camera’s main login screen. On Mac and Linux computers the browser defaults to MJPEG and you can see MPEG4 with a media player (e.g. QuickTime, VLC) if you open the RTSP stream for MPEG4.

MJPEG is Motion JPEG, basically a very quick sequence of images that resembles full motion video. However MJPEG has no sound and therefore on Mac and Linux computers you would use the media player (such as QuickTime or VLC) instead of the browser to access your camera if you want audio. The JPEG snapshot image is handy when you don’t want video or audio and just want a current picture.

Clicking on the “Secondary stream” and “Mobile stream” links will get you 2 more complete sets of URLs for your camera:

Secondary stream list

Intranet stream URL	
RTSP MPEG4 stream:	rtsp://192.168.0.21/live_mpeg4_1.sdp
RTSP MJPEG stream:	rtsp://192.168.0.21/live_mjpeg1.sdp
HTTP MPEG4 stream:	http://192.168.0.21/stream1.av
HTTP MJPEG stream:	http://192.168.0.21/stream1.jpg
HTTP ASF stream:	http://192.168.0.21/stream1.asf
HTTP snapshot image:	http://192.168.0.21/snapshot1.jpg
Internet stream URL	
RTSP MPEG4 stream:	rtsp://sharxdemo.servehttp.com:8150/live_mpeg4_1.sdp
RTSP MJPEG stream:	rtsp://sharxdemo.servehttp.com:8150/live_mjpeg1.sdp
HTTP MPEG4 stream:	http://sharxdemo.servehttp.com:8150/stream1.av
HTTP MJPEG stream:	http://sharxdemo.servehttp.com:8150/stream1.jpg
HTTP ASF stream:	http://sharxdemo.servehttp.com:8150/stream1.asf
HTTP snapshot image:	http://sharxdemo.servehttp.com:8150/snapshot1.jpg

Mobile stream list

Intranet stream URL	
Mobile 3GPP stream:	rtsp://192.168.0.21/live_3gpp.sdp
RTSP AMR audio stream:	rtsp://192.168.0.21/live_amr_audio.sdp
RTSP AMR audio stream:	rtsp://192.168.0.21/live_amr_audio.sdp
HTTP ASF stream:	http://192.168.0.21/stream2.asf
HTTP snapshot image:	http://192.168.0.21/snapshot_3gp.jpg
Internet stream URL	
Mobile 3GPP stream:	rtsp://sharxdemo.servehttp.com:8150/live_3gpp.sdp
RTSP AMR audio stream:	rtsp://sharxdemo.servehttp.com:8150/live_amr_audio.sdp
HTTP ASF stream:	http://sharxdemo.servehttp.com:8150/stream2.asf
HTTP snapshot image:	http://sharxdemo.servehttp.com:8150/snapshot_3gp.jpg

The reason for having multiple sets of streams is to allow simultaneous access to the camera at different resolutions without changing configuration. For instance, you could access one of the mobile streams from your cell phone and the Primary stream from your work computer, all without changing configuration and only by selecting the corresponding bookmark.

3GPP is a video format that is commonly used on cell phones and media players, including the free “Streamer” app for the iPhone. The 3GPP stream can show video with audio, using as little as 20K bandwidth.

Note that unless you sign up for a name for your camera and enter it in the DDNS section, your list of streams will only show numeric IP addresses. Also, if your router does not support UPnP, the external (internet) address won’t be shown here but will be available if you have set up the port forwarding.

Resetting the Camera back to Factory Settings

If you ever forget your admin password or have any other reason to reset the camera to its factory settings, please use the following procedure:

1) Make sure the camera is powered up

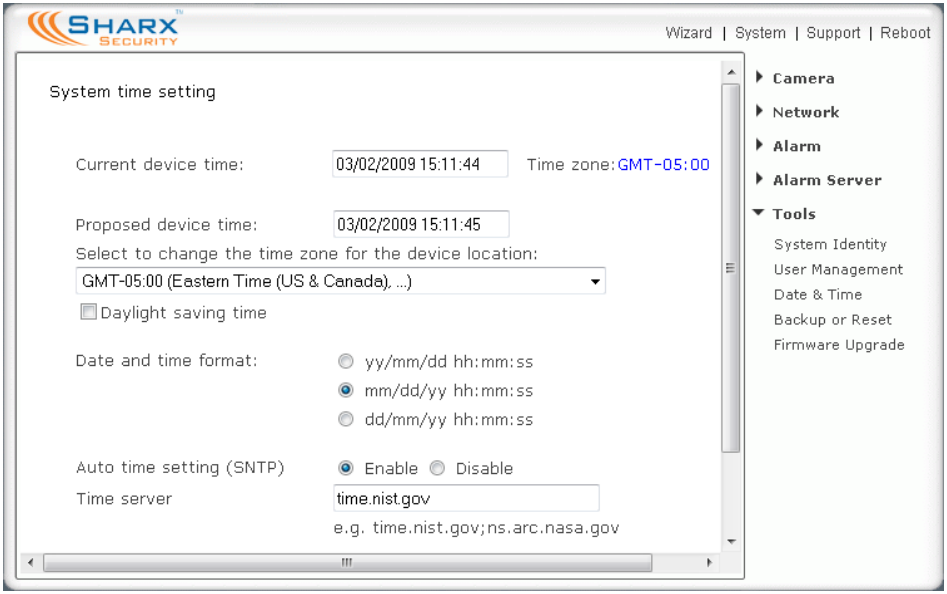
2) For indoor cameras insert the tip of a paper clip in the hole at the side of the camera to press the reset switch. You'll feel the click when the switch engages. For outdoor cameras it is easier to use the software reset function in the "Backup or Reset" menu. If hardware reset is needed, see the MicroSD card chapter for location of the reset switch.

3) Hold the switch down for 1 or 2 seconds, then let go. You'll see the power light go off for a few seconds. This indicates reset is in progress.

About 30 seconds later the camera will restart and is now at factory settings. Of course, after reset the username and password will both be "admin" again. (without quotes), and you may need to set current time zone as shown below.

Setting the Time and Time Zone

After a full reset you may want to make sure the correct time is set for your time zone. This is done automatically if the camera has internet access. Twice a year you will need to manually adjust the setting for "Daylight Savings Time".



SPECIFICATIONS	(subject to change without notice)
Camera	
Imaging Device	1/4" New generation CMOS sensor with color night vision
Pixels	310000
White Balance	Auto
Exposure Mode	Auto
Gain	Auto
Viewing Angle	Horizontal:60°, Vertical:45.0°
Focal Length	f=3.6mm
Aperture	F2.0
Min.llumination	1.0 Lux (SCNC2606 only). 2607, 2700, 3605/6 can see in total darkness with IR
Infrared LEDs	30 on SCNC2607, 28 on SCNC2700, 12 high power LEDs on SCNC3605 / 06 Automatic IR filter for excellent daytime colors on SCNC2700, SCNC3605/06
Network	
Image compression	MPEG4, JPEG, MJPEG, 3GPP
Image resolution	640x480(VGA), 320x240, 160x120, 176x144 (3GPP only)
Max. frame rate	Full 30fps @ 640x480 when viewing or recording with computer
Audio compression	AAC (40/32/24/16Kbps), AMR (4.75K – 12.2K)
Built-in microphone	Electret Condenser Microphone
Simultaneous viewers	Up to 10 depending on settings and available internet upload bandwidth
Authentication	ID/Password, Administrator/General User (Up to 64)
Network protocols	TCP,UDP,IP,ARP,ICMP,DHCP,DNS,HTTP,FTP,SMTP,NTP,UPnP,DDNS,RTSP,RTP
Stream types	HTTP, RTSP/RTP/RTCP, 3GPP
Network connection	Ethernet (10BASE-T/100BASE-TX) SCNC3606 and SCNC2700P: 802.11af PoE
Wireless LAN	
Wireless technology	IEEE802.11 b/g/n
Frequency	2.412-2.462GHz
Transmission speed	Up to 72 Mbps
Security	WEP (64/128 bit), WPA-PSK(AES/TKIP), WPA2-PSK(AES/TKIP)
General	
Power requirements	SCNC2606/07 DC 5V 2 Amps (international AC adapter included) SCNC2700, SCNC3605/06 DC 12V 1 Amp (international AC adapter included)
Power consumption	SCNC2606: 4W, SCNC2607, SCNC2700: 6W, SCNC3605/06: 8 W
Operating temperature	-5 to +45 °C (+22 to +113 °F) SCNC3605/06: -20 to +60 °C (-4 to +140 °F)
Storage temperature	-20 to +60 °C (-4 to +140 °F)
Operating humidity	20 to 80%RH (Non-condensing) SCNC3605/06: 0% to 100% (weatherproof)
Storage humidity	20 to 95%RH (Non-condensing) SCNC3605/06: 0% to 100% (weatherproof)
Dimensions(W x D x H)	SCNC2606, 07: 3.3" x 3.3" x 1.2" (85mm x 85mm x 30mm) SCNC2700: 3.4" x 3.4" x 1.3" (86 mm x 86 mm x 33 mm) SCNC3605, 06: 2.75" diameter x 8" long (70 mm diameter x 2000 mm)
Weight	SCNC2606: 5 oz / 135 g SCNC2607: 5.5 oz / 150 g (Main Body) SCNC2700: 6 oz / 166 g SCNC3605, 06: 30 oz / 850 g (Main Body)
Supplied accessories	AC adapter, CD-ROM, color matched mount or desktop stand (can be used as wall or ceiling mount), Cat5e cable
PC system requirements	
Operating system	Windows 7, VISTA, XP, Macintosh OSX Snow Leopard and Lion, Linux
Processor	Intel Pentium III, 1GHz or Higher (Multiple cameras require faster processor)
Memory	1 GB RAM Minimum
Web browser	Microsoft Internet Explorer Version 7.0 or later, Firefox, Safari, Chrome
Memory Card	MIcroSD and MicroSDHC capacities of 1 GB – 16 GB are supported

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, 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 the device.

Appendix A: Wireless setup instructions without Cat5

We have received inquiries from customers with no available wired network jack to plug the camera into for the initial configuration. For instance, if an Airport Express is used as the only router for a network, the single network jack is taken by the required connection to the cable or DSL modem. Or sometimes a camera is inadvertently mounted before wireless setup. Also, some 3G routers have no network jack at all.

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 Wifi network name (SSID) to:

   wirelessnc

   and 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) If you are using an Apple Airport Express, use the Airport utility 5.6 as shown on page 6 to reserve a fixed IP address for your camera using the camera's MAC address shown on the back of the camera.

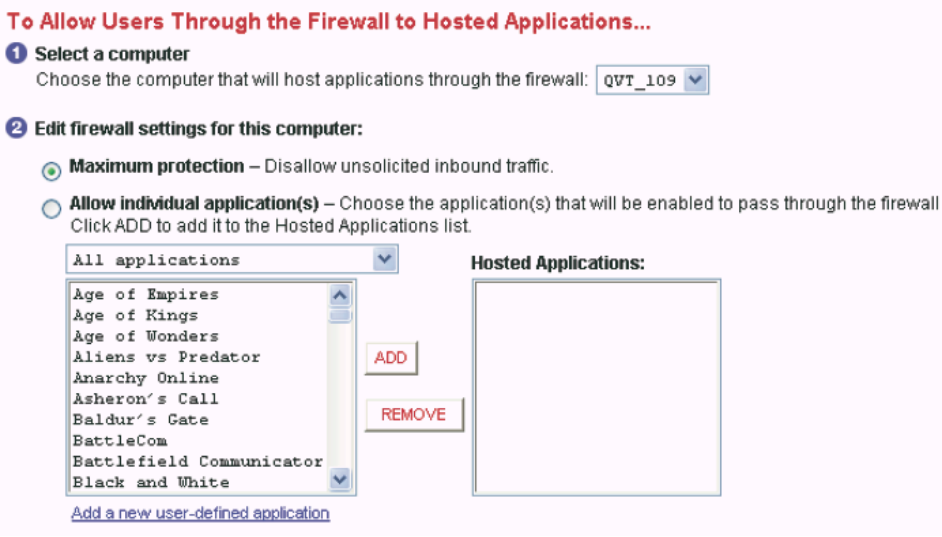
3) Power up the camera and wait about 1 minute… the camera should connect to your Wifi and you should be able to access it using the IP address that you reserved for it. If you have a Wifi router or access point other than the Airport Express, you can connect to your router and look in the DHCP clients list to see the IP address of the camera if it hasn't automatically announced itself with a UPnP popup window.

4) Now go to the camera's wireless setup menu, but don't use the "search" function. Type in the exact SSID that you had before the change in step 1, and type the exact password that you wish to use. After you hit "Apply", you won't be able to do further changes until the next step.

5) 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. You can now proceed with the setup of the camera as you should be able to see it at the same IP address as in step 3.

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 the SCNC2606 or SCNC2607 in the drop down box titled “Choose the computer…” and add these 2 applications so they are active for your camera, then you save the settings and restart your router.

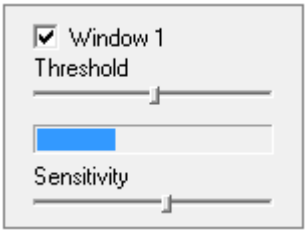
For the next camera, you call the first application Cam2HTTP and use public TCP port 8151 while still using “map to host” port 80. The second application would be Cam2RTP with UDP ports 30002-30003 and map-to-host port 30002.

Appendix C: Motion Detection Adjustment

After selecting “motion detection” from the main settings screen, you may need to expand the size of the display window towards the right to see the 4 controls for individual motion detection windows.

Each window can have individually adjustable sensitivity and threshold.

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.



Internet Explorer can show you a live indicator for motion: When there is motion, a blue level appears between the sensitivity and threshold slider as shown in the picture. More blue means more motion. To trigger an alarm (and hence send out emails 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.

If you do not use Internet Explorer you can adjust the settings by entering the desired coordinates for the windows. A window covering the entire 640x480 screen would cover 0-639 horizontally and 0-479 vertically, and this is the factory setting. (The numbers go to 639 and 479 because they start at 0, not 1) An example covering just the top half of the screen would use top left of 0,0 and bottom right 639, 239.

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 field of view of the camera through this motion detection menu for a while and make adjustments to threshold, sensitivity, and placement of the motion detection windows until you are pretty certain that you’ve tuned everything exactly right.

Please note that it generally does not make sense to define windows if the camera is not mounted securely. If it is just sitting on a desktop the slightest movement of the camera would invalidate your window positions.

Appendix D: Known issues

1. Recording multiple cameras on one NAS drive requires multiple network “shares”. A NetGear ReadyNAS and WD World Edition can set up multiple network shares but some lower end NAS drives cannot. The Apple Time Capsule shows only one share, but if you set up individual user accounts for each camera, then the Time Capsule automatically creates a share for each account and therefore can be used with multiple cameras, up to 4 cameras per Time Capsule.

2. If you use Gmail for motion detection and send a very large number of emails, Google may suspect that you are using the camera to send spam and may temporarily suspend or block your account. Use the schedule feature to get alerts only when you really want them, and use the interval time to suppress new emails for a given amount of time. We recommend at least 600 seconds (= 10 minutes).

3. Files recorded by the camera on MicroSD or NAS are in Apple QuickTime MOV format. Windows Media Player can play these files without audio. On both Mac and PC we recommend to install the latest Apple QuickTime Player 7 to play the files with video + audio.

4. 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. Therefore if you want to be able to access your camera from the internet you would have to uncheck this option.

5. Some wireless routers or access points have a feature called “wireless client isolation”. This is mainly for use in public networks where you want to prevent access from one wireless device to another. Do not use this feature or your router’s “guest network” if you want to access your camera from a laptop connected to same router.

6. D-Link DIR 655 and similar routers have to be at firmware 1.21 or later. If yours has version 1.10 firmware you need to upgrade your router.

7. Among all the wireless routers we tested, a few specific older models seem to have trouble initiating a wireless connection with our cameras: LinkSys WRT160N, 2wire 2701HG, old dome shaped Apple Airport. In this case we recommend upgrading to a newer router.

Appendix E: Burglar Alarm System Integration

The outdoor cameras in the SCNC36xx series have additional connectors to help with integration of the cameras into a complete burglar alarm system.

1: GND: Signal ground for use with DI
2: DI: Digital Input (use with GND)
3: DO: Digital Output (open collector)
4: Power + 12 VDC (MAX 0.4 A)

Typically this type of wiring is carried out by a professional security system installer. If you are not familiar with the terminology used here, please do not attempt to connect anything to this terminal block. Damage caused by improper wiring is not covered by warranty.

When the camera senses motion, and if the digital output is set to “Enable” in the camera’s “Digital I/O Setup” menu, it activates the digital output to trigger a burglar system. With a maximum load of 1 Amp and a maximum voltage of 60 V, this output has an open collector NPN Darlington transistor with the emitter connected to the GND pin. If used with an external relay a reverse polarity diode must be connected in parallel with the relay coil to protect against voltage transients. You would need to select a relay that uses less than 0.4A at 12V, and the relay and the diode would connect to pins 3 and 4.

Conversely, if the digital input is set to “Enable” in the camera’s “Digital I/O Setup” menu, a contact closure from DI to GND (pins 1 and 2) would trigger an alarm condition in the camera as if the camera’s own motion detection had triggered. This means that emails or FTP/HTTP uploads can be triggered or recording to MicroSD card can be initiated. Both the digital input and the camera’s motion detection can be active at the same time. If you only want this external input to trigger the camera’s alarms, you need to set all 4 motion detection windows in the “Motion Detection” menu to Disable (unchecked).

The round connector that looks similar to the power plug is for optional attachment of an amplified speaker system. This output is at line level similar to a computer speaker system. Using this, audio upload can be initiated from the microphone of a computer running Internet Explorer. There is no echo suppression, so if this is used it would make sense to turn down the camera’s own microphone.

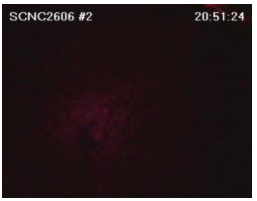
Appendix F: The SCNC2607 sees too much pink and purple!

The SCNC2606 has an optical filter element in the lens to remove all infrared light that cannot be seen by the human eye. This makes the remaining colors look rich and natural to us because we see colors the exact same way.

However, in order to see in total darkness, the SCNC2607 does not remove IR and therefore the SCNC2607 does not always see colors the way human eyes do. Depending on the scenery and the amount of naturally occurring IR light, the difference can be very slight, or there could be more of a pink / purple emphasis, or the colors could appear subdued and almost black and white.

The daytime colors on the SCNC2607 cannot be corrected by choosing a different setting. The only options are to use different lighting or to choose a camera model with automatic IR filter, such as SCNC2700 or SCNC3600 series.

To summarize the capabilities and color vision of the different models:

SCNC2606: Natural daytime colors but no infrared (cannot see at night)


SCNC2607: Weaker daytime colors but can see at night in total darkness


SCNC2700 and all SCNC3600 outdoor models: Excellent day and night vision

Our top of the line cameras have an automatic IR filter for natural daytime colors **and** IR night vision for the best in true day/night video performance.

Contact us

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

If you purchased this product from an authorized retailer in the USA you are eligible for priority email based technical support and up to 30 minutes of free phone based support per camera during the first 30 days after your purchase.

We are always glad to help, however we ask that you read the relevant sections of this manual first. If you still have questions please send us an email:

info@sharxsecurity.com

Most issues can be resolved very quickly. Even complicated issues are no problem for us. If you are totally stuck, we can make appointments for one-on-one telephone tech support tutorial until your camera is up and running.

Please keep in mind that remote access to your camera may require a few settings changes in your router, and that we cannot help you if you do not have your password for your own router. Also keep in mind that many routers (especially LinkSys and Dlink) have many versions of the firmware, and routers with older versions of the firmware probably need to be updated. Frequently this takes care of the most mysterious issues. Typically we do not schedule telephone tech support until your router firmware is at the latest version that is available from your router manufacturer's tech support web site. Please note that we cannot upgrade your router firmware. Please ask your router manufacturer for help with router firmware upgrades if needed.

We pledge that we will not let you fail. Contact us with any questions, no matter how simple or how complicated.