uniview

Better Security, Better World.

NETWORKING TUTORIALS

WORLD EYECAM

CONTENTS

LEARNING THE PORTS

Uniview has six recorder ports and three camera ports that can be used. All ports on Uniview devices are changeable and can be changed to anything within the proper networking port range of 1024-49151

The ports on a recorder can be found in the main menu under the network menu settings in the ports and port mapping sub menus.

Ports on cameras can be found and changed by logging directly into a camera on internet explorer by typing the cameras local IP address into the address (URL) bar. You can use the Uniview EZTools found on our website (worldeyecam.com) to find and change each cameras IP address.

RECORDERS

Recorders use a HTTP port (default 80), RTSP port (default 554), Media port (default 7070), SDK port (default 6060), HTTPS port (default 443), and ONVIF port (default 82).

New recorder firmware, from 6-1-2016 or newer, have combined the Onvif, Media, and SDK ports. Recorders with new firmware will only need the HTTP port and RTSP ports opened.

The HTTP port is used for accessing the recorder via the web browser and via the mobile app on android and iOS. This port is 80 be default but if needed to be changed is commonly changed to 8080. This port is used as your web protocol for the browser to direct network traffic to the correct server.

The RTSP port is used for streaming the recorders RTSP stream to a 3rd party program such as VLC player. This port is 554 by default which is the networking standard port for RTSP. This is 99% of the time going to stay at the default port. Please contact the network administrator at the location if you wish to use a different port.

The Media port is the recorders connection port. This is used to let the network allow the incoming connection and not block it to the recorder. The default port for media is 7070 this can be changed to anything within the 1024-49151 port range.

The SDK Port is used or connecting on the app. This is a back-end port used for making the connection from the app to the recorder. The default SDK port is 6060 but can be changed to anything within the proper port range.

Uniview units come with the option of using a secure HTTPS port for viewing on the web. This port using the default HTTPS port of 443 and if used clients will be required to have a signed certificate on their computer to view the recorder on the browser. This is good for banks, schools, and hospitals. 443 is the networking standard port used for HTTPS if you would like to use a different port please contact the locations network administrator.

Onvif port can be used to connect the recorder to a 3rd party VMS software that supports recorder or to a 3rd party device. This port is 82 by default but can be changed to be inside the proper network port range.

The recorders require that the HTTP port, Media port, and the SDK port to be open in the locations router in order for clients to fully connect to the unit via the phone, remote web browser, or remote computer using the EZStation. If you cannot do port forwarding at your location, please view our EZCloud introduction and tutorial.

CAMERAS

Cameras use a HTTP port (default 80), HTTPS port (default 443), and RTSP port (default 554).

The HTTP port is used for accessing the camera via the web browser and via the mobile app on android and iOS. This port is 80 be default but if needed to be changed is commonly changed to 8080. This port is used as your web protocol for the browser to direct network traffic to the correct server.

Uniview units come with the option of using a secure HTTPS port for viewing on the web. This port using the default HTTPS port of 443 and if used clients will be required to have a signed certificate on their computer to view the recorder on the browser. This is good for banks, schools, and hospitals. 443 is the networking standard port used for HTTPS if you would like to use a different port please contact the locations network administrator.

The RTSP port is used for streaming the cameras RTSP stream to a 3rd party program such as VLC player. This port is 554 by default which is the networking standard port for RTSP. This is 99% of the time going to stay at the default port. Please contact the network administrator at the location if you wish to use a different port.

If each individual camera is to be viewed remotely each camera will need a different HTTP & RTSP port and each camera will need to have its ports opened in the router for its own IP address. Cameras only need the HTTP and RTSP ports open to be viewed remotely.

HOW TO CHECK UNIVIEW PORT SETTINGS

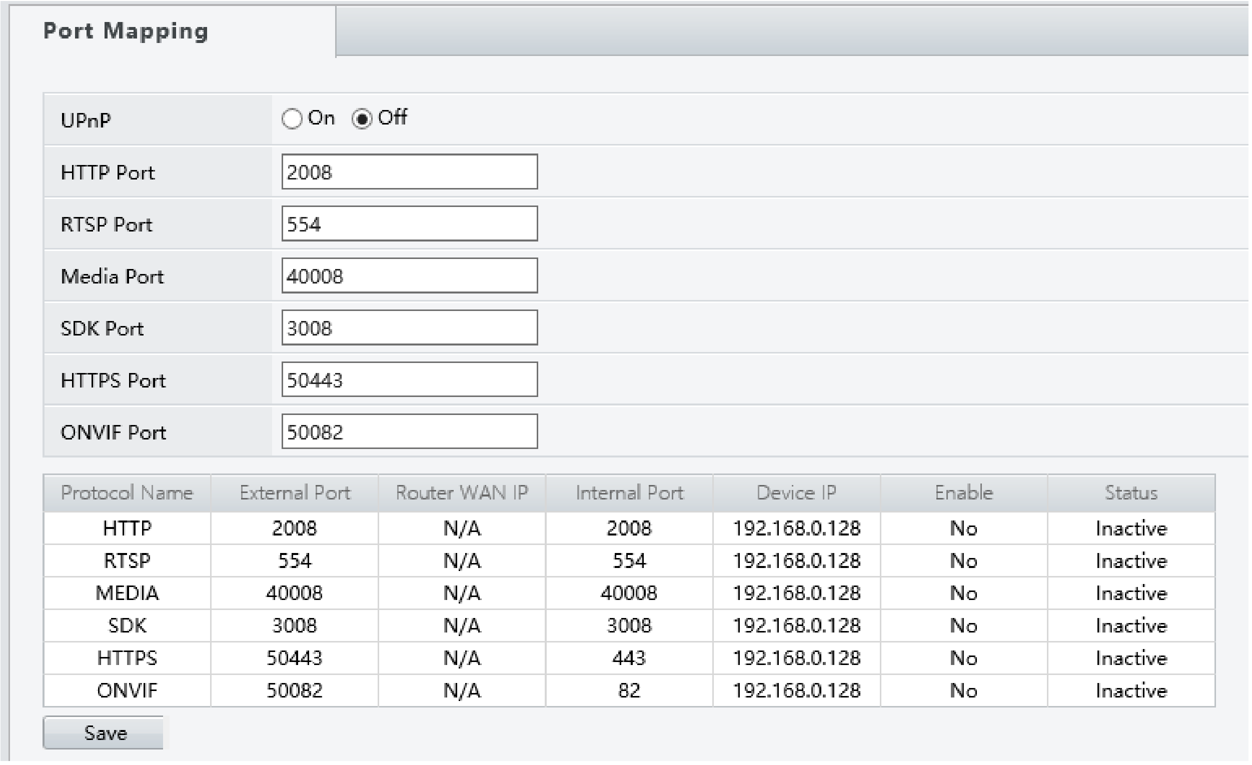
Uniview recorder come with Port Mapping (UPnP) enabled by default. UPnP is an automatic port forwarding feature that if also enabled in the router will open the recorders ports automatically.

The UPnP will open different external (access) ports than internal ports, this is for network safety. An example of this is port mapping will by default forward external port 50080 for http to the default internal port 80. When you use a port checking website to see if your ports are open you will need to check port 50080 and not 80 itself, and when viewing on the web or phone you will specify port 50080 and not 80.

All the port mapping rules can be changed so that the external port matches the internal port under the port mapping menu.

If the locations router does not have UPnP or you do not wish to use UPnP it can be disabled in the port mapping menu. Once UPnP is disabled you will need to manually port forward in the router and you need to make sure that your port mapping external ports match your internal ports to make putting in the port forwarding rules easy. See example below.

EXAMPLE 1:



Port Mapping

UPnP	○ On ● Off
HTTP Port	2008
RTSP Port	554
Media Port	40008
SDK Port	3008
HTTPS Port	50443
ONVIF Port	50082

Protocol Name	External Port	Router WAN IP	Internal Port	Device IP	Enable	Status
HTTP	2008	N/A	2008	192.168.0.128	No	Inactive
RTSP	554	N/A	554	192.168.0.128	No	Inactive
MEDIA	40008	N/A	40008	192.168.0.128	No	Inactive
SDK	3008	N/A	3008	192.168.0.128	No	Inactive
HTTPS	50443	N/A	443	192.168.0.128	No	Inactive
ONVIF	50082	N/A	82	192.168.0.128	No	Inactive

In this example UPnP is disable and is going to need manual port forwarding rules to be put into the router. In this situation you want to change your recorder External ports to match the internal ports.

In this example we have changed the needed ports to match the HTTP, RTSP, Media, and SDK ports. Now that the external ports and internal ports are the same we will be able to open the ports in the router with no problems.

The internal ports of the recorder can be changed in the "ports" menu. The "ports" menu contains the list of ports that your recorder is using on your network. All ports are explained in the first section of this tutorial

PORT FORWARDING IN YOUR ROUTER

Each network is going to be different and have different devices, most devices can be found on http://portforward.com/ with guides on how to open ports in them.

You can follow our general networking guide to learn the basics of port forwarding on networks with one or more router(s). Along with gathering the basic network information that you need to do the port forwarding along with information you can use to trouble shoot the port forwarding if it is not working

We suggest that after doing your port forwarding to check the ports on a website like canyouseeme.org or yougetsignal.com. If your ports are not open and you cannot find the problem, please call technical support.

WEC PORT FORWARDING GUIDE

Remotely accessing video recorders and cameras on the internet (WAN) is an important feature to most clients and it should be considered when installing and implementing a video surveillance system. Discussed on this page are three critical aspects of networking a video recorder or camera system:

- Port forwarding video recorder(s) and camera(s)
- Managing a network IP camera system
- Bandwidth and throughput limitations

Port Forwarding

Port forwarding is required to view a device across the internet (WAN) remotely. The most basic of implementations requires knowledge of the network layout and the log in information of all applicable routing devices. Here is a step by step process on how to network a video recorder:

1. Get a basic understanding of how the network is laid out. If the video recorder is behind multiple routers, ports must forward through all routers.

2. Find the gateway IP address of the routing device that the video recorder is attached to. If there is a Windows PC connected to the same network tier (router) as the video recorder, running a CMD from the start menu and typing the command **ipconfig** at the prompt will display the gateway information. On an Apple Mac computer, pull down the apple menu in the top left corner and click on System Preferences. Next click on Network under Internet and Network. The address will appear next to the Router heading. Also note the subnet mask.

3. Take note of the video recorder's IP address found in Main Menu > Setting > Network or by using the ConfigTool (Windows only). If the video recorder is set to DHCP, disable DHCP to allow the video recorder to keep a static (non-changing) IP address. By default, most video recorders are set statically at 192.168.1.108. If the gateway noted in the previous step is different (i.e. 10.1.10.1), change the gateway IP address in the video recorder to match the current network gateway and also change the IP address to match the gateway (i.e. 10.1.10.108). When changing the IP address of the video recorder, make sure that IP address is available by using the **ping** command in a CMD prompt (Windows) or Terminal (Mac). Also, in more uncommon situations, the subnet mask may also be different and may need to be changed to match the network.

4. Take note of the video recorder's HTTP and TCP ports (Main Menu > Setting > Network). The HTTP port is the web port used to view the video recorder (or camera) on web browsers and the TCP port is the port used for mobile devices (DMSS) and VMS software (PSS). By default, the HTTP port is 80 and the TCP port is 37777. If there is more than one video recorder to be forwarded through the same network, the IP address, HTTP and TCP ports must be different on each unit to differentiate them (i.e. 192.168.1.108 – 81 - 40001, 192.168.1.109 – 82 - 40002, etc.). Some ISPs do not allow for port 80 to be forwarded; in this case, the HTTP port should be changed on the video recorder and forwarded instead.
5. Access the router by inputting the gateway IP address noted in step 2, into a web browser. The router will usually ask for a username and password; if the log in information was changed from default, find out the credentials from the network administrator or internet service provider. Some of the more common default router log in combos are admin:admin and admin:password. Default router log in information can also be found on http://www.routerpasswords.com.

6. Once logged into the router, navigate to the Internet or Status section and find the IP address of the router. If the WAN IP address appears to look like a LAN IP (i.e. 192.168.x.x or 10.x.x.x), then another router is assigning this router an IP and the ports will need to be forwarded through both (see Multiple Router Port Forwarding section below for more details). Navigate to the Advanced section of the router and look for a Gaming/Applications, Port Forwarding, Pinholes or Virtual Servers menu. Sometimes the Port Forwarding menu can be in the Firewall section of the router as well. Every router brand and model is different, however there are two basic setups:
    1. The router allows for a set number of rules; in this case, select Custom Ports (rather than a preset port) if the option is available. For each rule, the router will usually ask for a private (internal) and public (external) port range. Use the same port for all entries. The rule will also have a protocol setting; set it to TCP. Enter in the local (LAN) IP address of the video recorder that corresponds to the port being forwarded. Make sure to save the port forwarding rules before navigating away from the menu.
    2. The router allows for port groups; in this case, a port group will have to be created and then assigned to an IP. When creating the group, name it something like “DVR_http” or “DVR_tcp”. On some routers, multiple port ranges can be added to the same group. After creating (and saving) the group, assign the group to the IP address of the video recorder. Save the port forwarding rules before navigating away from the menu.

7. After setting up the port forwarding rules, go to a website such as www.canyouseeme.org or www.yougetsignal.com/tools/open-ports/ to check and make sure that the ports are open. If the TCP port is open, but not the HTTP port, try changing the HTTP port to a number other than 80 or 8080 (i.e. 2000). If both HTTP and TCP are not open, try the following steps:
    1. Check the router for any firewall settings that could be blocking remote access. Every router makes and model is different when it comes to firewall settings.
    2. Try setting up a DMZ host. To do so, navigate to the Advanced (or Firewall) section of the router and look for a DMZ submenu. From here, enter in the local (LAN) IP address of the video recorder and save the settings. Sometimes the router will report that there are duplicate port forwarding rules, but this can be ignored. Test to see if the ports are open again. NOTE: The DMZ host only works for one device. The DMZ essentially opens all ports for that one device. Opening a DMZ presents a security vulnerability and the user may opt not to utilize this feature.
    3. If a DMZ host does not open the ports, then double check to make sure that the router is not behind another router(s). If it is, check the Multiple Router Port Forwarding section below.
    4. If the previous step does not apply, the ISP may be blocking all port forwarding. Call the ISP to find out more information on why port forwarding is not working properly on the routing device. If the client is using a satellite internet service, port forwarding may not work unless additional static IP addresses are purchased.

8. Once the correct ports are confirmed open, take note of the external IP address. The external IP address of the network can be found on www.ipcow.com (or on any of the port checking sites linked previously). The external IP address can be used to view the device remotely or a DDNS can be setup (more information on remote viewing provided below).

Multiple Router Port Forwarding

After reviewing the previous section, and it is discovered that there are multiple routing devices, take the following steps:

1. Note the routing device that the video recorder is currently attached to. Make sure that the computer used for network configuration is getting its network connection (IP address) from the same router. As in the previous section (Steps 2-5), access to the router should be done by inputting the router's gateway IP address into a web browser.

2. Log in to the router using the proper log-in credentials (see previous section step 5) and go to the Status or Internet menu of the router. Note the Internet IP address and Default gateway of the router. The IP address will be the dynamic IP address being issued by the router located

above the current router in the network structure. The gateway address will be used to access the higher tier router.

3. Forward the HTTP and TCP ports for the video recorder(s) IP address as described in the previous section.

4. Log in to the higher tier router using the Internet gateway address previously noted from Step 2.

5. Navigate to the Status or Internet menu of the higher tier router and inspect the Internet IP address and default gateway. Ensure that it has an address that is being assigned by the ISP either dynamically or statically. If it is another local IP address (i.e. 192.168.x.x or 10.x.x.x), then there may be a third router; this process will have to be repeated for each additional router.

6. Repeat the port forwarding steps 6 and 7 from the previous section, however the ports must be forwarded for the Internet IP of the lower tier router (rather than the local IP address of the video recorder)

7. Repeat step 7 from the previous section to check to see if the ports are open.

8. Repeat all steps from this section if there is any additional routers that the ports need to be forwarded through.

Managing a network IP camera system

Besides port forwarding, managing a network IP camera system requires changing device IP addresses to prevent conflicts, plotting out power over Ethernet (PoE) switches and cable distances. This next section will give some basic information on how to organize and maintain a network camera setup.

WEC recommends using a Windows PC so that the installer can use the ConfigTool to configure a new network IP camera system. If a Mac is used, a custom network must be created, and each camera must be attached and configured one at a time.

Configuring using the ConfigTool (Windows)

1. Download the ConfigTool here. Uncompress the ConfigTool.zip file and run the ConfigTool.exe application file. Allow the ConfigTool through any firewall alerts.

2. In the lower left-hand corner of the software, in the IP Version dropdown, select IPv4.

3. Click the Refresh button. The ConfigTool should now list all attached devices IP addresses.

4. With the latest firmware, the network IP cameras will be set to DHCP. If all the devices listed on the ConfigTool have different IP addresses, then the installer can move on to adding the cameras into the network video recorder(s) or VMS software.

5. If the cameras are all set to the default static 192.168.1.108, then they must be changed to different IP addresses that match the current network segment using the ConfigTool, double click a device listed in the program and log in. If the device is on a different segment than 192.168.1.1, then the program will request an IP address and default gateway change, otherwise it will log in. In either case, change the IP address to an available one on the LAN and make sure that the gateway and subnet mask is correct (matches the LAN settings).

6. Repeat step 5 on all cameras, ensuring each one has a different IP address. WEC suggests ordering the IP address to keep things organized. For example, 192.168.1.201, 192.168.1.202, 192.168.1.203 and so on.

7. If the client wants to access the cameras remotely, independently from a video recorder, then each camera must have differing HTTP and TCP ports. WEC suggests using 2xxx for the HTTP port and 40xxx for the TCP port (i.e. 2001 / 40001, 2002 / 40002, etc.)

Configuring using a Mac computer

1. First check to see if the cameras are set to DHCP by default. To do so, connect all cameras to the network and log in to the router using the default gateway. Most routers have a connected devices menu that will show all devices connected to the router and what IP addresses are being assigned. Check if the cameras are listed in the connected devices and try to log in to a few of the IP addresses using Safari. If the cameras are confirmed as set to DHCP, then no further camera configuration is needed.

2. If the cameras are not on DHCP, then a new network location must be created. Choose Apple menu > System Preferences, and then click Network. Choose Edit Locations from the Location pop-up menu, and then click Add (+). Enter settings for that match the network segment the cameras are on by default which is gateway 192.168.1.1, subnet 255.255.255.0 and the local IP of the Mac computer can be set to 192.168.1.2.

3. After setting up the new network location, connect one camera to the Mac. Usually this is done by connecting a PoE switch to the Mac's Ethernet port.

4. Using Safari, connect to the default static IP address of the camera – 192.168.1.108. Log in to the Web Service using the default credentials – admin: admin. Click the Setup tab and navigate to the Network menu on the left. Change the IP address, default gateway and subnet mask of the target network segment in the TCP/IP submenu. Be aware that after changing the information, the installer will not be able to access the camera on the custom network location, so make sure the information is correct.

5. Repeat step 4 for each camera, making sure that each IP address is unique and available on the target network segment.

Bandwidth and throughput limitations

When setting up a security camera system, the most frequent bottleneck to viewing performance is low bandwidth both on the LAN and WAN. This is especially true when working with network IP cameras. Low bandwidth can cause live video streams to appear staggered or lag, jumping between frames and missing seconds of footage. Here are some steps you can take to improve or troubleshoot bandwidth related issues:

LAN (Local Area Network)

- Lowering mainstream encode settings over all cameras can improve recordings if lag is experienced, however this can adversely affect image quality in both live streams and recorded footage. It is also suggested to change the bitrate to CBR (constant bitrate) if there is lag on recorded footage.

- All WEC video recorder units have 10/100/1000M (gigabit) uplink ports, however our network IP cameras do not. This means that when using multiple (8+) network cameras, it is suggested to use gigabit networking devices (switches and routers) when viewing them through a network video recorder. Using quality networking devices can drastically improve LAN performance.

- Many times, it is preferred to use a separate dedicated router for the camera system which can improve network load balancing and throughput management.

- Using Cat6 cabling may improve throughput, albeit minimally. Also, gigabit network devices (switches and routers) will be necessary to see any improvement from using higher quality network cabling.

WAN (Wide Area Network)

- When viewing remotely either through the Web Service, PSS or DMSS it is advised to use the extra stream. Extra stream is set to a low encode settings (resolution and bitrate) specifically for viewing remotely. Be aware, that extra stream does not have as good video quality as mainstream, so if higher quality is required for remote live viewing then lowering mainstream encode settings may be required.

- Generally, bandwidth and throughput is highly dependent on the internet service package the client is receives from their ISP. An improvement to remote viewing is made by increasing upload speeds, which means upgrading the whole package. WEC suggests at least 2MB upload speed per network camera, or around 25MB for a large camera system.

Other considerations

Here is a quick list of other factors that need to be considered when networking a security camera system:

- Specifications may require not recording at the location of the cameras. Remote recording can be accomplished with WEC video recorders. WEC suggests placing a video recorder at both the recording and the camera location to ensure network stability. To add the cameras remotely from the camera location's video recorder, it is as simple as using the external IP address and TCP port of the remote locations recorder and add it to the recording network video recorder as a remote device using the correct remote channel. For more information refer to this article.

- Certain WEC cameras are wireless (Wi-Fi) capable. Wi-Fi capability can be enabled by logging into the camera via the Web Service and setting up connectivity with the appropriate Wi-Fi routing device. For more information on Wi-Fi setup, refer to this article.