GUIDE TO PORT-FORWARDING FOR CAMERA CLOUDSHARE™

Videstra LLC
WWW.VIDESTRA.COM | CUSTOMER CONNECT: 608.999.9003

Legal

The information in this User's Manual has been carefully reviewed and is believed to be accurate. Videstra LLC assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates.

Note: For the most up-to-date version of this manual, please see our web site at www.videstra.com.

Videstra, LLC ("Videstra") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Videstra and/or its licensors, and is supplied only under a license.
Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

Videstra asserts that, upon initial delivery, all software and firmware are free of known viruses; however, Videstra accepts no responsibility for viruses, Trojan horses, Worms, Logic Bombs, Spyware or any malicious computer programs in the form of binary executable code, or scripts that cause harm to devices provided by Videstra or devices owned and operated within the end-user's control or facilities. It is the end-user's sole responsibility to provide adequate protection against all forms of malicious programs that can or do harm the end-user's ongoing business interests or property. Videstra will accept no responsibility for problems caused by changes to third party software (including updates, upgrades, downgrades and patches) on Videstra provided computers and devices.

IN NO EVENT WILL VIDESTRA, LLC BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. VIDESTRA, LLC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of the State of Wisconsin, USA. The State of Wisconsin, County of Dane shall be the exclusive venue for the resolution of any such disputes. The total liability for all claims against Videstra, LLC shall not exceed the price paid for the product.

Videstra® is a registered trademark, V-Manager, VestraView, Camera CloudShare and V-Streamer are trademarks used by Videstra, LLC.

Table of Contents

Port Forwarding

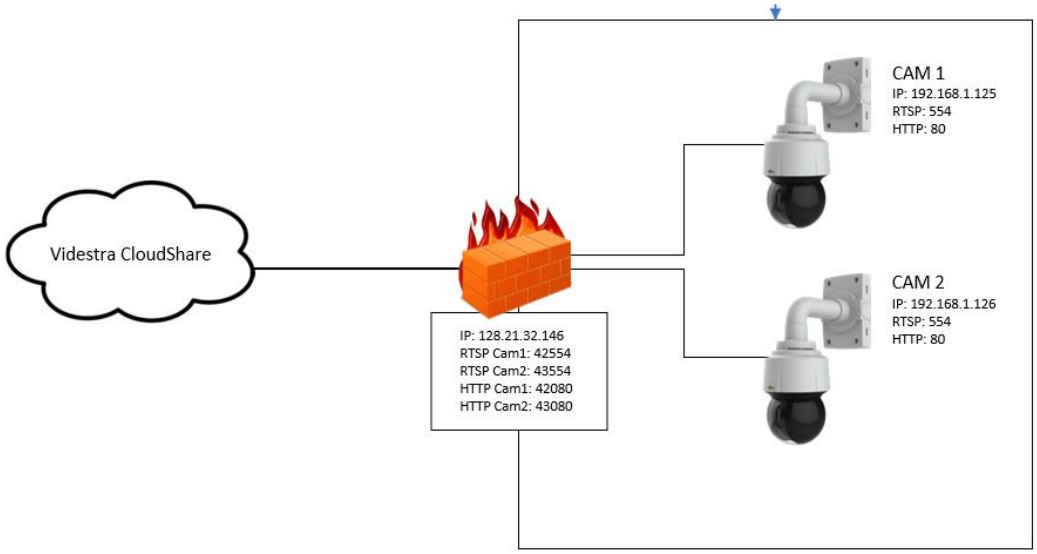
A Guide to getting your cameras onto the Videstra Camera CloudShare™

Why Port Forward

For the Videstra Camera CloudShare to work we need to allow an outside (public) service to connect to the camera(s) you want to share. This means the camera must either be on a public IP Address (see the chart in Appendix A), or two *incoming* ports must be opened to the camera. The port numbers are unimportant, but they must be open for TCP/UDP connections for the RTSP and HTTP protocols.

- Normally (default) RTSP is on port 554
- Normally (default) HTTP is on port 80

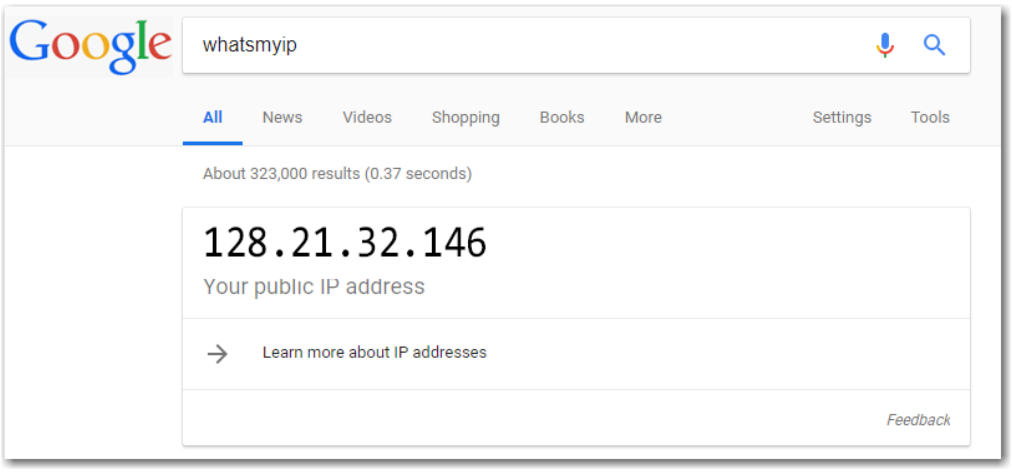
We do not recommend you forward these ports to the camera!
Instead it is much better to forward higher numbered ports to the camera such as 42554 and 42080. You can forward these ports to the default ports of the camera(s) IP Address.



In the graphic above we have *opened* the following ports on the local firewall: 42554, 43554, 42080 and 43080. The firewall will forward any *incoming* connection requests on these ports directly to the corresponding camera IP Addresses and ports.
This means that a request from *outside* the firewall at the public IP Address of 128.21.32.146 on port 42554 will be forwarded to Cam 1 at 192.168.1.125 on port 554.

Your Public IP Address

The *outside* public IP Address (128.21.32.146 in our example above) is your private networks *outside-facing* public address. If you have access to the Internet, you have an outside-facing public address. The easiest way to determine this address is to enter “WhatsMyIP” into a Google search.



The example above shows the result of a WhatsMyIP search on Google from inside a corporate firewall. Important: Make sure you do this search from the same network segment (subnet) as the camera(s) to which you will be port-forwarding. It's possible that the cameras are on a different subnet and reaching them may be on a different router/firewall with a different public-facing IP Address.

Setting up Firewall Rules

In order to successfully Port-Forward you will need full access to your firewall. This may be your main router or a separate firewall device. It depends on how your network is set up. Because there are many makes/models of routers/firewalls we cannot explain how to set up your router/firewall. The process ranges from super-complex to super simple. Here are some basic guidelines that will help:

- If your firewall rules let you set up *Single Port Forwarding* you will only need to enter a single port number you wish to forward to a camera
- You will need to set up a separate rule for each port you want to forward (in our example above you would need to set up 4 separate rules)
- If your firewall rules make you set up a *range* of ports to forward just set the range-start and range-end to the same number
- If your firewall lets you set up a forward rule for TCP, UDP or BOTH, set BOTH.
- If your firewall only lets you set up a rule for TCP or UDP then create two rules, one for TCP and one for UDP. RTSP works on both TCP and UDP. HTTP only works with TCP so you would only need to set one rule for HTTP – that being TCP.

What About Security

Opening *incoming* ports are anathema to most corporate IT managers. You may have difficulty getting this done. In some cases corporate IT will simply not allow this. If that is the case then cameras on your internal network will not be able to be shared through the Videstra Camera CloudShare. There are a few things you can do to "harden" the security of these open ports though.

Set up IP Filtering

IP Filtering will reject any connection request from non-white-listed IP Addresses. This means you can put the Videstra Camera Cloudshare IP Address into a table on your firewall and requests from anyone other than the Videstra Camera CloudShare service will be ignored. You can put in a number of IP

Addresses into the IP Filtering table if necessary, but typically only the Videstra Camera Cloudshare IP is necessary.

> *Note: The Videstra Camera CloudShare IP Address is different for each corporate customer. Contact Videstra to find out what your Camera CloudShare IP Address is.*

Never use default port numbers

As stated, Videstra recommends you do not forward ports 80 or 554 (default ports) to the camera(s) but instead move these external ports to parallel numbers such as 42554 and 42080.

Never set up a camera with default username/password

Always set secure usernames and passwords for cameras.

Don't worry too much

Hackers are after serious payloads (names, addresses, social security numbers, etc). Cameras have extremely little payload for any hacker. There is the danger that a hacker may subvert the camera to run other applications, but this is extremely unlikely. Simple IP Filtering will eliminate this danger altogether.

Appendix A – Private/Public IP Addresses

Class	Private IP Address Range	Public IP Address Range
Class A	10.0.0.0 – 10.255.255.255	1.0.0.0 – 9.255.255.255 11.0.0.0 – 126.255.255.255
Class B	172.16.0.0 – 172.31.255.255	128.0.0.0 – 172.15.255.255 172.32.0.0 – 191.255.255.255
Class C	192.168.0.0 – 192.168.255.255	192.0.0.0 – 192.167.255.255 192.169.0.0 – 223.255.255.255