

Source-Connect Network Configuration

Last updated May 2009



For further support:

Chicago: +1 312 706 5555

London: +44 20 7193 3700

support@source-elements.com

This document is designed to assist IT/Network administrators to configure your network to allow Source-Connect traffic in and out of your NAT or firewall protected network. It discussed Source-Connect and the supporting Q Manager service.

This document covers:

Notes

Required Network Configuration

Source-Connect / Q Manager Network overview

Using other UDP port numbers

How Source-Connect determines its network status

Common issues:

Connection Test: 'port not mapped' or 'failed'

Connection Test 'successful' however not able to connect with other users

Ports unable to be allowed due to company rules.

Anti-Virus is installed (generally Windows-only issue)

Notes:

1. 'local' means the internal static IP of the Pro Tools machine, e.g. 192.168.1.5, where the machine is behind NAT. If the Pro Tools machine is on DHCP, you should provide the machine with a static NAT IP first.

2. Source-Connect and the supporting Q Manager application establish two TCP connections, to source-elements.com on TCP ports 80 and 5222, using both HTTP and HTTPS. These connections must be allowed by the firewall or Source-Connect will return error #120 (connection to source-elements:80 not allowed) or #125 (connection to source-elements:5222 not allowed). Generally these connections are allowed by default except under the most strict circumstances. **You will only need to make changes to your TCP firewall rules if you get error #120 or #125 on logging in to Source-Connect.**

3. If you are analyzing network activity you may also note activity to your UDP port 5000. This can be ignored as it is conducting secondary network tests to enable operation of Source-Connect under less strict networks.

4. Source Elements software does not support any type of proxy at this time. It is important that the computer's public IP is the same IP that Source-Connect will send the UDP traffic to.

Required Network Configuration:

1. Either allow all outbound UDP ports, or allow outbound UDP connections to certain IPs as needed. Allow TCP connections to and from source-elements.com:80 and source-elements.com:5222 (generally this is allowed by default).

2. Port forward/map the following UDP ports to the local IP:

6000 – 6002

If the user has Source-Connect Pro, the above ports may be modified to preferred ports, between 1024 and 65535. The ports must be an even number plus the two ports immediately following, e.g. 10060 – 10062 or 25985 – 25988.

Source-Connect will use ports 6000–6001 (or the first 2 UDP ports you choose) and the Q Manager should be configured to use 6002 or the third UDP port you choose).

3. Ensure the firewall has been specified to allow inbound access on the three selected UDP ports.

Once you have done this, you can log in. Then, to check that your UDP ports are not firewalled and are mapped to your local IP, the status panel has a port status message.

- If the test comes back 'successful' (Pro) or 'open' (Standard), it means that the source-elements.com server is able to send and receive the UDP traffic.
- If you get 'port not mapped' it means that there is either a firewall or there is incorrect or absent port mappings for the UDP ports.
- If you get 'failed' then there is a firewall active on those ports for your local IP and/or your connection is going through multiple routers.

Source-Connect is peer to peer, and for the connection test to return successful you will need to allow outbound/inbound UDP from source-elements.com. Note that this rule is not necessarily required for successful operation of Source-Connect, it simply allows the user to be assured that the network is properly functioning. As long as the IP address of the connection partner you wish to use is enabled then Source-Connect will function as expected.

Note that we do not recommend setting your firewall rules to allow only to certain IP addresses. The IP of the source-elements.com server may change at any time. See the appendix for a list of current DNS and IP settings. This list is subject to change at anytime, however we will endeavor to provide 30 days notice.

Source-Connect Network Overview

Source-Connect transfers a real-time, high-quality audio stream between remote locations via the UDP protocol. UDP is used in order to allow low delay communication, and thus relies on direct or unfirewalled network access to UDP ports.

Generally, the machine running Source-Connect is on a private network address (behind NAT, or Network Address Translation). UDP is unable to independently negotiate NAT, so the network (secured by a router and/or firewall) must generally be configured with specific Port Mapping (or Port Forwarding) rules.

If for some reason Port Mapping is not possible, e.g. the user has no administration access to the network, Source-Connect will attempt to negotiate the network. Negotiation, if possible at all, is much slower to connect and can create unwelcome delays and data loss because the UDP data must traverse an unknown and possibly temporarily available path. And, when this negotiation attempt simply attempt fails, the user cannot receive the audio stream. In addition, if the ports are not mapped Quality of Service rules cannot be applied.

Therefore, we recommend to all users that in a permanent studio situation they administer the network appropriately to allow proper UDP port mapping.

Q Manager Network Overview

The Q Manager will by default also use UDP as it's transfer mechanism in a similar manner to Source-Connect Pro, however the volume of data is generally much lower as it is used to transfer only data that may have been lost during the Source-Connect recording session. The Q Manager is also configurable to use FTP instead of UDP.

See the Q Manager guide in the Source-Connect manual for assistance on this matter or contact Support.

Using other UDP port numbers:

Source-Connect allows the user to specify a particular set of UDP ports. First, the user must configure their internal network settings to connect via a static IP, rather than DHCP, and then configure port mapping on the router.

For example, the user configures the router to forward all incoming UDP data on ports 6000 and 6002 to their internal IP address, and enters the number 6000 in the Settings Panel of Source-Connect. (Ports may be any even number between 1024 – 65534 and this number plus two)

How Source-Connect logs in and determines its network status

1. Source-Connect first determines the internal(private/local) and external (public) IP addresses. The external IP address is determined by sending an HTTP request to a remote application on our server, source-elements.com:80.
2. A connection is now established with source-elements.com:5222. This is a persistent connection and will remain open for the duration of the Source-Connect session. If this connection is broken Source-Connect will respond with an error and log the user out.
3. Source-Connect determines the port mapping status by sending an HTTP request to our source-elements.com to begin forwarding a series of test UDP packets to the specified ports (e.g 6000, 6001, 6002) on the determined IP address.

If Source-Connect receives these test UDP packets, it knows that port mapping is enabled, and will use these ports for the incoming audio stream.

If Source-Connect does not receive any of the UDP packets, it will time-out and inform the user that the test has either returned '**port not mapped**' or '**failed**'. In the case of 'port not mapped', Source-Connect may have detected an alternative method of connecting and it is still possible that the user will receive an incoming stream. Usually an outgoing stream is still possible in this case. If 'failed' it is highly unlikely that there will be sent or received audio.

Common issues: Connection Test: 'port not mapped' or 'failed'

The user is able to properly configure their network for UDP port mapping however the connection test does not return successfully.

Possible causes:

- The user's ISP will filter HTTP traffic on port 80
- The user is behind a HTTP proxy
- All TCP and/or UDP ports are firewalled
- The ISP is using a caching server for UDP traffic

In these cases Source-Connect will not be able to determine the user's public IP address, and the test UDP packets will be 'lost' within the ISP's network. The test will not return successful, and the secondary, less reliable methods will be used where possible.

Common issues: 'successful' however not able to connect with other users

The user has 'successful' or 'open' for the port status, however no connections are possible with other users. In this case the 'receive' light on the Status panel will not be blinking and no audio signal is received.

Possible causes:

- The network is blocking ***all*** incoming traffic on UDP ports **except** from source-elements.com (hence the successful connection test)
- A local firewall is on the machine

Common issues: Ports unable to be allowed due to company rules.

In many cases under a corporate network the UDP ports cannot be fully opened. In this case you have several options:

- 1.** Obtain the IP address of the connecting user and allow inbound traffic from this IP address. This IP address should ideally be static (as provided by the ISP) so it does not change for your next session. You can contact Support for testing as we have a static IP available.
- 2.** Install a second internet connection, e.g. consumer-strength cable or DSL. This method works very well, especially if the line is dedicated to Source-Connect, and will ensure all traffic is completely separate from the corporate network.
- 3.** Use any VPN connection, e.g. IPSEC or PPTP. This works extremely well and can be configured in various ways for usability. Contact our Support team for advice.
- 4.** Windows-only systems may choose to use a service like Hamachi, which is supported by Source-Connect Pro.

Common issues: Anti-Virus is installed

Generally this is a Windows-only issue. Source-Connect may be considered by some AV software as being a threat and the AV software will not allow the inbound connection. Either configure your AV software to allow Source-Connect and Q Manager connections, or disable the AV software during use.