

SciFinder[®] Security and the Internet

SciFinder is a TCP/IP (Transmission Control Protocol/Internet Protocol) client/server product that uses the Z39.50 communications protocol. Z39.50 is an application-level information search and retrieval protocol used primarily by on-line services. The registered port for Z39.50 is Port 210.

1. How secure is SciFinder through my company's firewall?

It is recognized that any communication passing through a firewall is a potential concern to the organization behind the firewall, so SciFinder has been designed to be firewall-secure:

- The SciFinder client initiates all communications. During periods of client inactivity exceeding several minutes, the server will poll the client, across the already established Z39.50 connection, requesting confirmation that the client is still active. Other than the exception mentioned, the SciFinder server only acts in response to client requests. The SciFinder server will never initiate a connection to a client. Port 210 may remain in "stealth mode" when "viewed" from the Internet.
- All communications take place on a registered port: 210. If firewall and client modifications are required by your network security requirements, we strongly recommend that port 210 is used as the designated Z39.50 port on your firewall
- All client communications are with a pair of well-known CAS servers
 - 134.243.85.3:210
 - 134.243.85.4:210
- The 2006 SciFinder client is configured, by default, to use 134.243.85.3 for all communications. The SciFinder 2007 client uses both IP addresses and it implements a 'random chooser' in the client to provide for load balancing and redundancy. CAS strongly recommends that both IP addresses be allowed in firewall rules.
- Firewall security may be strengthened by using rule sets that allow Port 210 outbound traffic only to the two IP addresses listed above.

2. What about IP spoofing?

A network attack in which a "bad" computer is configured to masquerade as a "good" computer is called IP spoofing. For a spoof to be successful, a rogue computer must be able to convince clients that it is the target (good) computer. The more customized a network service is, the more difficult it is to spoof. For this reason, IP spoofing attacks have always targeted general network services such as "telnet", and not highly unique services such as the Z39.50 protocol which is used by the SciFinder client and server for application level communications. Additionally, the goal of a spoof is to attack a computer by exploiting network "trust" in a client/server relationship ("trust" in a network context means that one side of a client/server connection implicitly trusts the other side and so does not require the other side to authenticate itself). SciFinder does not use network trust, making it a poor target for a network spoof.

3. Are my communications private?

To enhance data confidentiality, SciFinder never sends plain-text ASCII data. All network communications are encoded using BER (Basic Encoding Rules). BER performs a translation ("scrambling") of data. Both sides of a SciFinder client/server connection BER-encode their data just prior to sending it. The receiving side decodes the data by inverting the translation.

More information about the Z39.50 protocol is available at its Maintenance Agency Home Page at the Library of Congress:

<http://lcweb.loc.gov/z3950/agency>

SciFinder BLAST (Nucleotide and Protein Searching) Security

SciFinder BLAST searching launches client software written in SUN[®] Java. The client – server communications use HTTPS (SSL) with 128 bit encryption via Port 443.

- The client will attempt to create a secure tunnel via Port 443 through the firewall to the BLAST server at:
 - 134.243.5.42:443 DNS name: <https://scifinder.cas.org>
- The client may be configured to use an HTTP proxy server by running the "Site Preference Editor" within SciFinder and entering HTTP Proxy internal connection information into the HTTP Networking section.
 - Consult the Site Administrator Guide or
 - Contact CAS Customer Care at
 - help@cas.org
 - 1-800-753-4427 in North America
 - 614-447-3700 worldwide.
- Client authentication to the HTTP proxy is supported using Basic Authentication.

How can we increase the security of our connection to SciFinder?

CAS offers Business to Business VPN connections for companies wishing to increase the security of their Internet connection to CAS. Your SciFinder sales representative can provide additional information. The Business to Business VPN will require a VPN gateway at the company Internet interface compatible with the CAS CISCO VPN concentrator. The CAS networking and security staff will coordinate setup of the VPN tunnel with your IT staff.

Do you need further information or assistance with SciFinder networking configuration?

- Contact CAS Software Support Team at
 - ssd@cas.org
 - 1-800-753-4427 in North America — Choose VoiceMenu Option #4
 - 614-447-3700 worldwide — Choose VoiceMenu Option #4
 - Toll-Free SciFinder Support from Europe

Belgium	0800-7-1238	France	0800-90-3061
Germany	0800-181-9365	Switzerland	0800-89-6083
United Kingdom	0800-89-1590		