Frequently Asked Questions about Open Proxies and JSTOR

---

1. What is a proxy server?

A proxy server is a computer running software which allows it to operate as a "middle-man" between a workstation on a network and the Internet. The proxy server relays information between a workstation and an Internet site. In effect, the server in this situation is acting as a "proxy" for the workstation. Proxy servers are commonly used to improve performance for web users by temporarily caching webpages and to provide remote access to licensed resources by relaying requests from authorized remote users through the IP of the proxy. Proxy servers can also be used to log Internet use and block access to prohibited sites. One result of connecting to an Internet resource through a proxy server is that the destination resource or website cannot identify the address of the originating workstation - only the IP of the proxy server is apparent.

2. What is an open proxy?

Proxy servers are extremely useful when configured correctly and are perfectly acceptable as long as measures are in place to ensure that only authorized users are allowed to access them.

Many machines on the Internet, however, are running proxy servers set up without proper access restrictions and are therefore "open" proxies. An "open" proxy is available to relay requests from anyone on the Internet. For example, when a student or faculty member sets up a web server on his or her computer, a proxy server might also be installed by default. Without special configuration, these proxy servers often have no access restrictions in place. If the computer is within a range of IP addresses that have access to JSTOR, then the result is that literally anyone in the world can use that proxy server to enter JSTOR, as well as other licensed electronic products and restricted campus resources. It is important to note that this is not a fault of any

institution or library, but a weakness inherent in the current system of using IP addresses for authentication to restricted resources.

3. **Why can't JSTOR simply deny open proxies?**

Once we know that a computer is running an open proxy, we can deny access to the archive from its IP address. However, it is not easy to determine which computers are running open proxy servers. While we can check an individual computer in a few minutes, there are currently hundreds of thousands of IP addresses that have access to the archive. Unfortunately, it is impossible for us to proactively check each one to see which are running open proxies and which are not.

In addition, even if we had the ability to test all authorized IP addresses, this action could be construed as a breach of security on many campuses. It could trigger alarms on those computer networks which have intrusion detection systems in place to prevent wholesale scanning of IP numbers, which is a common tactic used by hackers to find open proxies. If you have any questions about this, please contact support@jstor.org.

4. **What is JSTOR's process for suspending access to an open proxy?**

Because malicious and unauthorized downloading is often automated and rapid, it may not always be possible for us to notify you before we need to take action. In the event that we have to suspend access to an IP number on your campus which is running an open proxy server, though, please be assured that we will alert our designated JSTOR contacts as soon as we possibly can. If you would like to know who the designated contacts are for your campus, please contact support@jstor.org

5. **Our library currently has or is in the process of setting up a proxy server. What do we need to watch out for?**

In our experience, it is very rare to find an institutional proxy that has been set up without proper access restrictions in place. The vast majority of the unrestricted proxy servers we have encountered have not been main campus proxies set up to accommodate access for authorized users to library resources. Rather, these unrestricted proxies tend to be unintentionally established by individuals affiliated with an institution who install web servers on their personal workstations for other purposes. In doing so, they unknowingly provide an open access point to their university's network.

6. **Is dial-up access to a campus network vulnerable?**

Dial-up access is generally quite secure when users are required to enter a username and password. Since their user names and passwords are generally connected to their email accounts, users have some incentive to protect this information.

7. **How do I determine if there has been unauthorized use of JSTOR through our campus network?**

We will contact the participating institutions from which we experience high numbers of unauthorized downloads. If you would like to confirm that no unauthorized activity has taken plan on your campus, please contact support@jstor.org and our technical staff will examine your site records.

8. **How can we scan our networks for open proxies?**

There are a number of port scanning tools that can be used to identify open proxy servers, but your best resource for locating open proxies is likely to be your campus network staff. If you do find a tool that you want to run yourself, we highly recommend that you contact network staff prior to running it, since running a port scanner on your campus network could possibly trigger network alerts.

9. **Does JSTOR offer password accounts as an alternative to IP-based authentication?**

At this time, JSTOR does not offer password accounts as an authentication option for academic institutions, except in specific limited circumstances. One difficulty with password accounts is that JSTOR cannot verify individuals' affiliations with participating sites. There is currently no standard way for libraries or their institutions to communicate to us who the individuals are that make up their faculty, staff and students. While some resource providers offer one or two password accounts that are shared among users at individual institutions, our experience has been that this method presents different, but significant, security problems. For example, passwords can be easily and quickly shared with unaffiliated users, or easily posted to a public web page.

If you have additional questions or suggestions, please contact support@jstor.org.

Last updated on February 3, 2008