Control FirstSearch sessions

Learn how to control how FirstSearch sessions work for your library users. FirstSearch uses a cookie to end any existing FirstSearch session whenever another FirstSearch session is started on the same workstation. For libraries that purchase a specified number of ports (simultaneous logons) as part of their FirstSearch access, this feature releases ports for use by other users more quickly than if the existing session was left to time out.

What is the purpose of this feature?

A growing number of libraries add links to their Web pages that lead directly to individual databases within FirstSearch. A user may click one of these links to access a FirstSearch database and start a FirstSearch session. After searching the database, the user might click the browser's Back button to return to the library's Web pages without exiting FirstSearch and ending the session. Then the user might click another link to access another FirstSearch database and start another session. This leaves an extra FirstSearch session open until the end of its specified timeout period. The user may access several databases in this way, leaving several sessions open.

By ending any existing FirstSearch session whenever another FirstSearch session is started on the same workstation, this feature increases the number of available ports for libraries with a specified number of ports. This helps control the number of ports that libraries need to purchase.

How does this feature work?

If this feature is turned on:

- FirstSearch checks for an existing cookie each time a new session is started.
- If the cookie exists, FirstSearch ends the session identified in the cookie and stores the session ID of the new session.
- Or, if the cookie does not exist, FirstSearch simply writes and stores a cookie containing the session ID of the new session.

Which FirstSearch access methods does this feature affect?

This feature affects only Web browser access to FirstSearch. It does not affect Z39.50 access.

Does this feature have privacy or security issues?

The cookie used by this feature is a small data file written and stored on a workstation's hard drive each time a
FirstSearch session is started. The only data that the file contains is the ID code that FirstSearch assigns each time a session is started. This session ID contains no information about the user, workstation, or library.

However, if you allow your browser to accept this FirstSearch cookie, it will also accept cookies from other Web sites. If your library's browsers do not accept cookies now, consult your system administrator before changing that browser setting.

**How can we turn this feature off or on?**

**On by default**

If your browser accepts cookies, this feature is turned on unless you turn it off. You do not need to make any changes in order to benefit from this feature.

If your browser does not accept cookies, you must set it to accept them in order to benefit from this feature. Consider possible privacy or security issues before changing the setting.

**Turning it off**

You can turn this feature off using any of the following methods:

- Set your browser not to accept cookies.
- If you use IP address recognition, add onesession=no as a component of your IP address recognition URLs.

**Browser settings.** Consult your system administrator if you need assistance setting your browser not to accept cookies.

**IP address recognition.** The following is an example of an IP address recognition URL that includes the component to turn off the feature:

```plaintext
https://firstsearch.oclc.org/fsip?dbname=worldcat&onesession=no
```

**Who can help us with this feature?**

Contact OCLC Support if you need assistance with this feature, or see the documentation for IP address recognition.