Servlets and Sessions

## Jsessionid

JSESSIONID is **a cookie generated by Servlet containers and used for session management in J2EE web applications for HTTP protocol**. If a Web server is using a cookie for session management, it creates and sends JSESSIONID cookie to the client and then the client sends it back to the server in subsequent HTTP requests.

### [Automatic Parameterization of JSESSIONID Cookie Values](https://www.loadtestingtool.com/help/jsessionid-cookie-values.shtml" \l ":~:text=JSESSIONID%20is%20a%20cookie%20generated,server%20in%20subsequent%20HTTP%20requests.)

## How to create a cookie?

**How to create Cookie?**

1. Cookie ck=new Cookie("user","sonoo jaiswal");//creating cookie object.
2. response.addCookie(ck);//adding cookie in the response.

## HTTP location header field:

https://en.wikipedia.org/wiki/HTTP\_location

The **HTTP Location** [header field](https://en.wikipedia.org/wiki/HTTP_header) is returned in responses from an [HTTP](https://en.wikipedia.org/wiki/HTTP) [server](https://en.wikipedia.org/wiki/Server_(computing)) under two circumstances:

1. To ask a web browser to load a different web page ([URL redirection](https://en.wikipedia.org/wiki/URL_redirection)). In this circumstance, the Location header should be sent with an [HTTP status code](https://en.wikipedia.org/wiki/HTTP_status_code) of 3xx. It is passed as part of the response by a web server when the requested [URI](https://en.wikipedia.org/wiki/URI) has:
   * Moved temporarily;
   * Moved permanently; or
   * Processed a request, e.g. a POSTed form, and is providing the result of that request at a different URI
2. To provide information about the location of a newly created resource. In this circumstance, the Location header should be sent with an HTTP status code of [201 or 202](https://en.wikipedia.org/wiki/List_of_HTTP_status_codes#2xx_success).[[1]](https://en.wikipedia.org/wiki/HTTP_location#cite_note-RESTful_Web_Services-1)

## PD-S-Session-id

 A different **PD**-**S**-**SESSION**-**ID** cookie is generated for unauthenticated **sessions**, **sessions** in process of authentication, and authenticated **sessions**.

<https://community.ibm.com/community/user/security/communities/community-home/digestviewer/viewthread?GroupId=2863&MessageKey=ca1c2694-1d21-4808-b871-064911323c94&CommunityKey=e7c36119-46d7-42f2-97a9-b44f0cc89c6d&tab=digestviewer&ReturnUrl=%2Fcommunity%2Fuser%2Fibmz-and-linuxone%2Fgroups%2Fnewtoz%2Fntz-discussions>

In a situation where I have an authenticated web session with both PD-S-SESSION-ID & PD-ID cookies set on the browser, when a call to pkmslogout is done, is it normal that I receive a "Set-Cookie: PD-ID=; Max-Age=0; Domain=blahblah; Path=/; Expires="Sun, 01-Jan-1995 01:00:00 GMT"; Secure; HttpOnly" for the PD-ID but nothing for the PD-S-SESSION-ID?

If so, I am Assuming that the session represented by the PD-S-SESSION-ID is nevertheless invalidated in ISAM. What would be the simplest most direct way to proove this? Is there a way to question ISAM directly on the status of a session giving it the value of the PD-S-SESSION-ID token?

Trying to access a protected ressource triggers ISAM to refuse the access to the ressource and send back another set-cookie for PD-S-SESSION-ID but with a different value. Am I right in assuming that this new PD-S-SESSION-ID represents a (new) unauthenticated session?

also, if required is there a setting that would force ISAM to send a "Set-Cookie: PD-S-SESSION-ID=; Max-Age=0;" similar to the one for PD-ID when pkmslogout is used? And why is that not the case by default, any issues/draw back to this that I am not seeing?

### Configuring session cookie names

https://www.ibm.com/docs/en/sva/9.0.6?topic=sharing-configuring-session-cookie-names

The cookie name used for WebSEAL session cookies is specified by the **tcp-session-cookie-name** and **ssl-session-cookie-name** stanza entries in the **[session]** stanza of the WebSEAL configuration file. For example (default WebSEAL cookie names for TCP and SSL sessions):

[session]

tcp-session-cookie-name = PD-H-SESSION-ID

ssl-session-cookie-name = PD-S-SESSION-ID

### Configuring DNS domains

<https://www.ibm.com/docs/en/sva/9.0.6?topic=configuration-standard-webseal-junctions>

[session-cookie-domains]

domain = example.com

domain = abc.ibm.com

## setHeader(), addHeader()

## What if the user doesn’t accept cookies?