
How to Configure Session Tracking

<https://campus.barracuda.com/doc/4259862/>

Session Tracking

A Session refers to all requests a single client makes to a server. A session is specific to the user and for each user a new session is created to track all requests from that user. Every user has a unique session identified by a unique session identifier. Session Tracking enables the Barracuda Web Application Firewall to limit the number of sessions originating from a particular client IP address in a given interval of time. Limiting the session generation rate by client IP address helps prevent session-based Denial of Service (DoS) attacks. To configure Session Tracking use **WEBSITES > Advanced Security** and choose **Edit** from **Options**. Specify the desired session protection fields:

- **New Session Count** – Maximum number of new sessions allowed per IP address; Range: 1 - 65535; Default: 10.
- **Interval** – The time in seconds for which the number of sessions cannot exceed the **New Session Count** setting; Range: 1 - 6000 seconds; Default: 60.
- **Session Identifiers** – The token type used to recognize sessions. Choose from the list, or see **Configuration of Session Identifiers** to add a Session Identifier.
- **Exception Clients**: List clients which are exempted from this protection. IP address ranges should be separated by a "-" (hyphen). Multiple ranges or IP addresses can be listed with "," (comma) separation. The list should not contain overlapping IP address ranges.
- **Status** – Set to *On* to enable session tracking.

After configuring the above fields, click **Save**.

Configuration of Session Identifiers

Configuring session identifiers allows the Barracuda Web Application Firewall to recognize session information in requests and responses. To create a new session identifier, perform the following steps:

1. Go to the **ADVANCED > Libraries > Session Identifiers** section.
2. Locate the desired identifier and click **Edit**, or to add a new identifier, click **Add Session Identifiers**.
3. Enter or modify the session **Identifier Name**. This name will appear in the list of Session Identifiers from which you choose when you configure **Session Tracking**.
4. Enter or modify the following session token parameters: **Token Name**, **Token Type**, **Start Delimiter**, **End Delimiter**. For example, "JSESSIONID=12345;" would be configured with session **Token Name**: JSESSIONID, **Token Type**: Parameter, **Start Delimiter**: = and **End Delimiter**: ; to allow Barracuda Web Application Firewall to successfully extract the Session ID

12345.

5. Newly added or edited Session Identifiers appear in the Session Identifiers list on the **Edit Session Tracking** page when you choose the **Edit** option on the **WEBSITES > Advanced Security > Session Tracking** section.

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.