Log Retention and Location

https://campus.barracuda.com/doc/14938/

Barracuda WAF-as-a-Service generates four types of logs:

- **Access Logs** contain a record of each HTTP/HTTPS request processed by Barracuda WAF-as-a-Service.
- **Firewall Logs** contain a record of each policy violation found by Barracuda WAF-as-a-Service, along with the associated action performed by Barracuda WAF-as-a-Service.
- **Event Logs** contain a record of specific network activity, including events related to Certificate, DDoS, or DNS.
- **Audit Logs** contain a record of actions taken by the service Users, the System, Barracuda Support Technicians, and Engineering Operators.

Note that in some circumstances, a single HTTP/HTTPS request might generate more than one Firewall Log entry. For example, if Block Attacks is turned off, multiple violations might be detected in the same request and logged, but because none of them cause the request to be blocked, Barracuda WAF-as-a-Service continues processing and finds more violations.

You can interact with these logs in multiple ways:

- View the Access, Firewall, and Event logs in the Logs page for an application. See Access, Firewall, and Event Logs.
- View Audit logs for the account in the AUDIT LOGS tab. See Audit Logs.
- Export as a CSV file, on-demand from the Logs page. See Access, Firewall, and Event Logs, and Audit Logs.
- Retrieve via the Barracuda WAF-as-a-Service API.
- Export in real time via the Syslog or Azure EventHub, using the **Log Export** component. For more information, refer to Log Export.

Access, Firewall, and Event Logs are retained for 30 days for Advanced WAF-as-a-Service plans and 60 days for Premium WAF-as-a-Service plans, and 45 days for Legacy Licenses. Audit logs are retained for 180 days. After this time period the logs are deleted automatically. If you require longer retention, be sure to download or retrieve your logs using one of the above methods before they are automatically deleted.

If you require longer retention, be sure to download or retrieve your logs using one of the above methods before they are automatically deleted.

If you have specific data residency requirements, be sure to select deployment locations that meet those requirements, as described in Understanding Deployment Locations. Your traffic will only be processed in the locations you select.

© Barracuda Networks Inc., 2026 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.