Logs Overview

The Barracuda Web Application Firewall has a comprehensive logging feature to record significant events. Events related to HTTP traffic, actions of the Barracuda Web Application Firewall, and user actions are captured in logs. These log messages enable a system administrator to:

- Obtain information about the Barracuda Web Application Firewall traffic and performance.
- Analyze logs for suspicious activity.
- Troubleshoot problems.

The following types of logs are available in the Barracuda Web Application Firewall:

- Web Firewall Logs
- Access logs
- Audit logs
- System Logs
- Network Firewall Logs

Each log in **Web Firewall Logs**, **System Logs** and **Network Firewall Logs** is associated with a log level that indicates the severity of the log. An administrator can configure the severity level based on the error messages/information that needs to be recorded in the logs. You can export the logs in .csv format and save the file to your desktop using **Generate CSV File** and **Download CSV File** options.

Log Levels

- 0-Emergency – System is unusable (highest priority).
- 1-Alert – Response must be taken immediately.
- 2-Critical – Critical conditions.
- 3-Error – Error conditions.
- 4-Warning – Warning conditions.
- 5-Notice – Normal but significant condition.
- 6-Information – Informational message (on ACL configuration changes).
- 7-Debug – Debug-level message (lowest priority).

In This Section: