Log Export

https://campus.barracuda.com/doc/79462622/

Barracuda WAF-as-a-Service generates various types of logs, as described in Log Retention and Location. The Log Export component enables you to export these logs in real time via the Syslog protocol or Azure event hubs. You can then stream the data from Azure event hubs to SIEM (Security Information and Event Management) tools, like Splunk, ArcSight, and others.

Before You Begin

Regardless of how you will export your logs, be sure to allow the source IPs for the export logs, as described in Restricting Direct Traffic .

- 34.227.174.172
- 40.71.30.40

Choose one of the following methods to export logs:

- Exporting to Syslog
- Exporting to Azure Event Hubs

Exporting to Syslog

Preparing to Export Logs

To export logs, you must have a Syslog server. You can set up your server or use a server provided by a cloud service.

- If you are running syslog on a UNIX machine, ensure you start the syslog daemon process with the *-r* option so it can receive messages from external sources.
- Windows users require additional software when using syslog, because the Windows OS does not include the syslog capability. There are many syslog solutions available, both free and commercial, including Kiwi Syslog.
- If you are using a cloud service, they will provide you with the server hostname, port, and protocol. Barracuda WAF-as-a-Service can export logs via UDP, TCP, or SSL protocols.

Syslog Facility

Syslog receives different types of log messages. To differentiate and store them in distinct log files, log messages contain a logging priority and a logging facility, in addition to the actual message and IP address.

There are eight facility options. All log messages are marked with one of the facility options, labeled **local0** through **local7**. By default, each syslog server is marked with **local0**.

For each configured syslog server, you can associate a specific facility with each log type, so your syslog server can segregate the log of each type into a different file.

See the instructions below for setting a facility option.

> You can set the same facility for both Firewall Logs and Access Logs.

Severity Level

You can set the severity level to export firewall logs and system logs to the configured export log server(s). Barracuda WAF-as-a-Service severity levels, listed from greatest to least severity, are:

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice – Default setting
- Information
- Debug

Notice is the default setting, indicating normal, but significant conditions.

Barracuda WAF-as-a-Service exports logs based on the selected severity level. For example, if you set the severity to **Critical**, then logs with a severity level of **Critical** and above (that is, **Emergency**, **Alert**, and **Critical**) are all sent to the external log server.

Configuring Export Log Information

1. Within Barracuda WAF-as-a-Service, open the application. In the left navigation panel, select **Log Export**.
2. Click **Add Export Log Server**.
3. In the **Add Export Log Server** page, specify the following information:

- **Name** – Enter a name for the new setting.
- **Log Server Type** – Select **Syslog NG**.
- **Server Address and Port** – Add the IP address or Hostname and Port for the external log server. The port is automatically entered based on your selection in **Connection Type** below.
- **Connection Type** – Select how you will connect with the external log server. Based on your selection, the appropriate port is automatically entered in the **Server Address and Port** field, located directly above.
- **Syslog Header** – Select a standard header or select Custom to specify the header.
- **Firewall Logs** – Specify the export format for Firewall Logs. This typically matches the type of logging server to which you are exporting logs. The following log formats are displayed in the drop-down list:
  - **Default** - The default firewall logs format defined by the Barracuda WAF-as-a-Service.
  - **CEF:0 (ArcSight)** – The Common Event Format (CEF) log used by ArcSight.
  - **HPE ArcSight CEF:0** - The Common Event Format (CEF) log used by HP ArcSight. This is the updated version of CEF:0 (ArcSight).
  - **LEEF1.0 (QRadar)** – The Log Event Enhanced Format (LEEF) log used by QRadar.
  - **Microsoft Azure Log Analytics** - The default log format used by Microsoft Azure Log Analytics.
  - **Symantec SIM** – The default log format used by Symantec SIM.
  - **RSA enVision** – The default log format used by RSA envision.
  - **Splunk** – The default log format used by Splunk.
  - **Custom** – Define a custom log format using the values displayed in the Log Field Macros.
    If you do not see your log type listed, select **Custom** and enter the format. See below for the format specifier. If you do not want to export Firewall Logs, select **Do Not Export**.
    - **Severity** – Select the severity for log events you want to export. Events with that severity, and higher levels of severity, are exported. The default setting is **Notice**, described above.
    - **Facility** – Specify where you want to store the log file, so logs are kept separate and are easy to retrieve. See Syslog Facility.
- **Access Logs** - Specify the export format for Access Logs. This typically matches the type of logging server to which you are exporting logs. The following log formats are displayed in the drop-down list:
  - **Default** - The default access logs format defined by the Barracuda WAF-as-a-Service.
  - **Common Log Format** – The default format for logged HTTP information.
  - **NCSA Extended Format** – The Common Log Format appended with referer and agent information.
  - **W3C Extended Format** – The default log format used by Microsoft Internet Information Server (IIS).
  - **CEF:0 (ArcSight)** – The Common Event Format (CEF) log used by ArcSight.
  - **HPE ArcSight CEF:0** - The Common Event Format (CEF) log used by HP ArcSight. This is the updated version of CEF:0 (ArcSight)

- **LEEF1.0 (QRadar)** – The Log Event Enhanced Format (LEEF) log used by QRadar.
- **Microsoft Azure Log Analytics** - The default log format used by Microsoft Azure Log Analytics.
- **Symantec SIM** – The default log format used by Symantec SIM.
- **RSA enVision** – The default log format used by RSA enVision.
- **Splunk** – The default log format used by Splunk.
- **Custom** – Define the custom log format using the values displayed in Log Field Macros.
  If you do not see your log type listed, select **Custom** and enter the format. See below for the format specifier. If you do not want to export Firewall Logs, select **Do Not Export**.
- **Facility** - Specify where you want to store the log file, so logs are kept separate and are easy to retrieve. See Syslog Facility.

◦ Event Logs – Specify the export format for Event Logs. This typically matches the type of logging server to which you are exporting logs. The following log formats are displayed in the drop-down list:

- **Default** - The default event logs format defined by the Barracuda WAF-as-a-Service.
- **Custom** - Define the custom log format using the values displayed in Export Log Formats.
  If you do not see your log type listed, select Custom and enter the format. See below for the format specifier. If you do not want to export Firewall Logs, select Do Not Export.
- **Facility** – Specify where you want to store the log file, so logs are kept separate and are easy to retrieve. See Syslog Facility.

4. Click **Add** to add the above settings.

Exporting to Azure Event Hubs

To use Azure Event Hubs, contact Barracuda Networks Technical Support.

Configuring Export Log Information for Azure Event Hubs

Exporting log data to Azure event hubs enables you to analyze that data with third-party SIEM (Security Information and Event Management) tools. For more information, refer to this Microsoft document, Stream Azure monitoring data to an event hub or external partner.

1. Within Barracuda WAF-as-a-Service, open the application. In the left navigation panel, select **Log Export**.
2. Click **Add Export Log Server**.
3. In the **Add Export Log Server** page, specify the following information:

- **Name** – Enter a name for the new setting.
- **Log Server Type** – Select **Azure Event Hubs**.
- **Event Hub Name** – Specify the name of your Azure event hub.
- **Service Bus Name** – Specify the name of the service bus for your Azure event hub.
- **Policy Name** – Specify the policy name for your event hub.
- **Policy SAS Key** – Specify the Microsoft Azure event hub SAS key value.
- **Send Traffic Logs** – Enable to export traffic logs.
- **Send WAF Firewall Logs** – Enable to export Barracuda Web Application Firewall logs.
- **Send WaaS Event Logs** – Enable to export Barracuda WAF-as-a-Service event logs.

4. Click **Add** to add the above settings.

Log information is automatically sent to your Azure event hub, and beyond if you choose.

Default Log Format for Firewall Logs

The default log format for Firewall Logs:

%t %un %lt %sl %ad %ci %cp %ai %ap %ri %rt %at %fa %adl %m %u %p %sid %ua %px %pp %au %r %uid

Example:

```
Apr 13 08:05:07 Barracuda - 2024-04-13 08:05:07.183 +0000 57fbcbf54f-z6pxk WF
ALER TILDE_IN_URL 213.182.115.22 35245 10.125.7.107 31200 security-policy
GLOBAL DENY NONE PathInfo="~" GET /index.html TLSv1.2 curl/7.47.0
10.145.7.147 60148 12ed42d1bef-365b5f9
```

Description

The following table provides information about each element of the firewall log for the above example:

Field Name	Example	Description
Time	Apr 13 08:05:07	Data and time of the log when it was generated.
Unit Name	Barracuda	Name of the unit.
Log Type	WF	Type of log: Web Firewall Log, Access Log, or Event Log.

Severity Level	ALER	Defines the seriousness of the attack. Values: • EMERGENCY – System is unusable (highest priority). • ALERT – Response must be taken immediately. • CRITICAL – Critical conditions. • ERROR – Error conditions. • WARNING – Warning conditions. • NOTICE – Normal but significant condition. • INFORMATION – Informational message (on ACL configuration changes). • DEBUG – Debug-level message (lowest priority).
Attack Description	TILDE_IN_URL	Name of the attack triggered by the request.
Client IP	213.182.115.22	IP address of the client sending the request.
Client Port	35245	Port associated with the client IP address.
Application IP	10.125.7.107	IP address of the application that receives the traffic.
Application Port	31200	Port associated with the application IP address.
Rule ID	security-policy	Name of the policy to which the Barracuda WAF-as-a-Service matched the request.
Rule Type	GLOBAL	Indicates the type of rule that was hit by the request that caused the attack. The following is the list of expected values for Rule Type: • Global – indicates that the request matched one of the global rules configured under Security Policies. • Global URL ACL – indicates that the request matched one of the global URL ACL rules configured under Security Policies. • URL ACL – indicates that the request matched one of the Allow/Deny rules configured specifically for the given website. • URL Policy – indicates that the request matched one of the Advanced Security rules configured specifically for the given website. • URL Profile – indicates that the request matched one of the rules configured on the URL Profile. • Parameter Profile – indicates that the request matched one of the rules configured on the Parameter Profile. Header Profile – indicates that the request matched one of the rules configured on the Header Profile.
Action Taken	DENY	The appropriate action applied on the traffic. • DENY – denotes that the traffic is denied. • LOG – denotes monitoring of the traffic with the assigned rule. • WARNING – warns about the traffic.
Follow Up Action	NONE	The follow-up action as specified by the action policy. It can be either None or Locked in case the lockout is chosen.

Attack Details	PathInfo="~"	Details of the attack triggered by the request.
Method	GET	HTTP method used by the request. Values: GET, POST, HEAD, etc.
URL	/index.html	URL specified in the request.
Protocol	TLSv1.2	Protocol used for the request.
Session ID	-	Value for this field remains *blank*.
User Agent	curl/7.47.0	The value contained in the User-Agent request header. Normally, this information is submitted by the clients, which details the browser, operating system, software vendor, or software revision, in an identification string.
Proxy IP	10.145.7.147	If the client requests are coming through a proxy or gateway, then this field provides the IP address of the proxy.
Proxy Port	60148	The port of the proxy server whose IP address has been logged in the Proxy IP field above.
Authenticated User		The username of the currently authenticated client requesting the web page.
Referer		The value contained in the Referrer HTTP request header. It identifies the web resource from which the client was “referred” to the requested URL.
Unique ID	12ed42d1bef-365b5f9	ID generated for the request. A unique ID is generated for every log.

Default Log Format for Access Logs

The default log format for Firewall Logs:

%t %un %lt %ai %ap %ci %cp %id %cu %m %p %h %v %s %bs %br %ch %tt %si %sp %st %sid %rtf %pmf %pf %wmf %u %q %r %c %ua %px %pp %au %cs1 %cs2 %cs3 %uid

Example:

```
Apr 13 08:05:07 Barracuda - 2024-04-13 08:05:07.183 +0000 57fbcbf54f-z6pxk TR
10.225.7.211 12290 112.122.137.66 34225 "-" "-" GET TLSv1.2
app201452.azurelab.cudawaas.com HTTP/1.1 404 8011 107 0 0 10.36.45.24 443 0
INTERNAL DEFAULT PROTECTED INVALID /index.html/?name=srea
http://10.99.109.2/index.cgi namkrl=sreask curl/7.47.0 10.221.7.155 60168
Peter curl/7.47.0 "-" app201452.azurelab.cudawaas.com 16ed45d1bef-486b5f9
```

Description

The following table provides information about each element of the access log for the above example:

Field Name	Example	Description
Time	Apr 13 08:05:07	Date and time of the log when it was generated.
Unit Name	Barracuda	Name of the unit, which is same as the default hostname.
Log Type	TR	Type of log: Web Firewall Log, Access Log, or Event Log.
Application IP	10.225.7.211	IP address of the application that receives the traffic.
Application Port	12290	Port associated with the application IP address.
Client IP	112.122.137.66	IP address of the client sending the request.
Client Port	34225	Port associated with the client IP address.
Login ID		Login ID used by the client when authentication is set to On for the application.
Certificate User		Username as found in the SSL certificate when Client Authentication is enforced by the Barracuda WAF-as-a-Service.
Method	GET	HTTP method used by the request. Values: GET, POST, HEAD, etc.
Protocol	TLSv1.2	Protocol used for the request.
Host	app201452.azurelab.cudawaas.com	IP address of the host or website accessed by the user.
Version	HTTP/1.1	HTTP version used by the request.
HTTP Status	404	The standard response code that helps identify the cause of the problem when a web page or other resource does not load properly.
Bytes Sent	8011	Bytes sent as a response by the Barracuda WAF-as-a-Service to the client.
Bytes Received	107	Bytes received from the client as a part of the request.
Cache Hit	0	Specifies whether the response is served out of the Barracuda WAF-as-a-Service cache or from the backend server. Values: 0 – if the request is fetched from the server and given to the user. 1 – if the request is fetched from the cache and given to the user.

Time Taken	0	Total time taken to serve the request from the time the request landed on the Barracuda WAF-as-a-Service until the last byte given out to the client.
Server IP	10.36.45.24	IP address of the backend web server.
Server Port	443	Port associated with the backend web server.
Server Time	0	Total time taken (in milliseconds) by the backend server to serve the request forwarded to it by the Barracuda WAF-as-a-Service.
Session ID	-	Value for this field remains *blank*.
Response Type Field	INTERNAL	Specifies whether the response came from the backend sever or from the Barracuda Web Application Firewall. Values: INTERNAL, SERVER.
Profile Matched Field	DEFAULT	Specifies whether the request matched a defined URL or Parameter Profile. Values: DEFAULT, PROFILED.
Protected Field	PROTECTED	Specifies whether the request went through the Barracuda WAF-as-a-Service rules and policy checks. Values: PASSIVE, PROTECTED, UNPROTECTED.
WF Matched	INVALID	Specifies whether the request is valid. Values: INVALID, VALID.
URL	/index.html	URL of the request without the query part.
Query	name=srea	Query part of the request.
Referer	http://10.99.109.2/index.cgi	The value contained in the Referrer HTTP request header. It identifies the web resource from which the client was “referred” to the requested URL.
Cookie	namkrl=sreask	Cookie as found in the HTTP request headers.
User Agent	curl/7.47.0	The value contained in the User-Agent request header. Normally, this information is submitted by the clients, which details the browser, operating system, software vendor or software revision, in an identification string.
Proxy IP	10.221.7.155	If the client requests are coming through a proxy or gateway, this field provides the IP address of the proxy.

Proxy Port	60168	The port of the proxy server whose IP address has been logged in the Proxy IP field above.
Authenticated User	Peter	Username of the currently authenticated client requesting the web page.
Custom Header 1	curl/7.47.0	The header name for which you want to see the value in the Access Logs.
Custom Header 2	-	The header name for which you want to see the value in the Access Logs.
Custom Header 3	app201452.azurelab.cudawaas.com	The header name for which you want to see the value in the Access Logs.
Unique ID	16ed45d1bef-486b5f9	ID generated for the request. A unique ID is generated for every log.

Log Field Macros

When defining the custom format, use the macros mentioned in the table to insert various fields in the log entry.

Log Field Macros for Web Firewall Logs

Web Firewall Logs	Description
%ai - Application IP	IP address of the application that receives the traffic.
%ap - Application Port	Port associated with the application IP address.
%at - Action Taken	The appropriate action applied on the traffic. • DENY – denotes that the traffic is denied. • LOG – denotes monitoring of the traffic with the assigned rule. • WARNING – warns about the traffic.
%ad - Attack Description	Name of the attack triggered by the request.
%adl - Attack Details	Details of the attack triggered by the request.
%ag - Attack Group	Name of the attack group as categorized by Barracuda WAF-as-a-Service based on the violations/attacks.
%aid - Attack ID	Predefined ID assigned to the attack.
%au - Authenticated User	Username of the currently authenticated client requesting the web page.
%ci - Client IP	IP address of the client sending the request.
%cp - Client Port	Port associated with the client IP address.
%fa - Follow-up Action	The follow-up action as specified by the action policy. It can be either None or Locked in case the lockout is chosen.
%seq - Log ID	A unique ID generated for the log.

%lt - Log Type	Type of log: Web Firewall Log, Access Log, or Event Log.
%m - Method	HTTP method used by the request. Values: GET, POST, HEAD, etc.
%p - Protocol	Protocol used for the request.
%px - Proxy IP	If the client requests are coming through a proxy or gateway, this field provides the IP address of the proxy.
%pp - Proxy Port	The port of the proxy server whose IP address has been logged in the Proxy IP field above.
%r - Referer	The value contained in the Referrer HTTP request header. It identifies the web resource from which the client was “referred” to the requested URL.
%ri - Rule ID	Name of the policy to which the Barracuda WAF-as-a-Service matched the request.
%rt - Rule Type	Indicates the type of rule that was hit by the request that caused the attack. The following is the list of expected values for Rule Type: • Global – indicates that the request matched one of the global rules configured under Security Policies. • Global URL ACL – indicates that the request matched one of the global URL ACL rules configured under Security Policies. • URL ACL – indicates that the request matched one of the Allow/Deny rules configured specifically for the given website. • URL Policy – indicates that the request matched one of the Advanced Security rules configured specifically for the given website. • URL Profile – indicates that the request matched one of the rules configured on the URL Profile. • Parameter Profile – indicates that the request matched one of the rules configured on the Parameter Profile. Header Profile – indicates that the request matched one of the rules configured on the Header Profile.
%sid - Session ID	Value for this field remains *blank*.
%sl - Severity Level	Defines the seriousness of the attack. Values: • EMERGENCY – System is unusable (highest priority). • ALERT – Response must be taken immediately. • CRITICAL – Critical conditions. • ERROR – Error conditions. • WARNING – Warning conditions. • NOTICE – Normal but significant condition. • INFORMATION – Informational message (on ACL configuration changes). • DEBUG – Debug-level message (lowest priority).
%t - Time Stamp	The time recorded in the following format: "yyyy-mm-dd hh:mm:ss.s" (one or more digits representing a decimal fraction of a second) TZD (time zone designator, which is either Z or +hh:mm or -hh:mm)
%u - URL	URL specified in the request.

%ua - User Agent	The value contained in the User-Agent request header. Normally, this information is submitted by the clients, which details the browser, operating system, software vendor, or software revision, in an identification string.
%un - Unit Name	Name of the unit.
%uid - Unique ID	ID generated for the request. A unique ID is generated for every log.

Log Field Macros for Access Logs

Access Logs	Description
%ai - Application IP	IP address of the application that receives the traffic.
%ap - Application Port	Port associated with the application IP address.
%au - Authenticated User	Username of the currently authenticated client requesting the web page.
%br - Bytes Received	Bytes received from the client as a part of the request.
%bs - Bytes Sent	Bytes sent as a response by the Barracuda WAF-as-a-Service to the client.
%ch - Cache Hit	Specifies whether the response is served out of the Barracuda WAF-as-a-Service cache or from the backend server. Values: 0 – if the request is fetched from the server and given to the user. 1 – if the request is fetched from the cache and given to the user.
%cu - Certificate User	Username as found in the SSL certificate when Client Authentication is enforced by the Barracuda WAF-as-a-Service.
%ci - Client IP	IP address of the client sending the request.
%cp - Client Port	Port associated with the client IP address.
%c - Cookie	Cookie as found in the HTTP request headers.
%ct - Client Type	Specifies the type of client making the request. Values: • Whitelist Bot • Fake Bot • Bot • Attack Bot • Attack • Unknown
%cs1 - Custom Header 1	The header name for which you want to see the value in the Access Logs.
%cs2 - Custom Header 2	The header name for which you want to see the value in the Access Logs.
%cs3 - Custom Header 3	The header name for which you want to see the value in the Access Logs.
%cs4 - Custom Header 4	The header name for which you want to see the value in the Access Logs.

%cs5 - Custom Header 5	The header name for which you want to see the value in the Access Logs.
%cs6 - Custom Header 6	The header name for which you want to see the value in the Access Logs.
%h - Host	IP address of the host or website accessed by the user.
%s - HTTP Status	The standard response code that helps identify the cause of the problem when a web page or other resource does not load properly.
%id - Login ID	Login ID used by the client when authentication is set to On for the application.
%seq - Log ID	A unique ID generated for the log.
%lt - Log Type	Type of log: Web Firewall Log, Access Log, or Event Log.
%m - Method	HTTP method used by the request. Values: GET, POST, HEAD, etc.
%p - Protocol	Protocol used for the request.
%pf - Protected Field	Specifies whether the request went through the Barracuda WAF-as-a-Service rules and policy checks. Values: PASSIVE, PROTECTED, UNPROTECTED.
%px - Proxy IP	If the client requests are coming through a proxy or gateway, this field provides the IP address of the proxy.
%pmf - Profile Matched Field	Specifies whether the request matched a defined URL or Parameter Profile. Values: DEFAULT, PROFILED.
%pp - Proxy Port	Port of the proxy server whose IP address has been logged in the Proxy IP field above.
%q - Query	Query part of the request.
%r - Referer	The value contained in the Referrer HTTP request header. It identifies the web resource from which the client was “referred” to the requested URL.
%rtf - Response Type Field	Specifies whether the response came from the backend server or from the Barracuda WAF-as-a-Service. Values: INTERNAL, SERVER.
%sid - Session ID	Value for this field remains *blank*.
%si - Server IP	IP address of the backend web server.
%sp - Server Port	Port associated with the backend web server.
%st - Server Time	Total time taken (in milliseconds) by the back-end server to serve the request forwarded to it by the Barracuda WAF-as-a-Service.
%t - Time	Date and time of the log when it was generated.
%tt - Time Taken	Total time taken to serve the request from the time the request landed on the Barracuda WAF-as-a-Service until the last byte given out to the client.
%u - URL	URL of the request without the query part.

%ua - User Agent	The value contained in the User-Agent request header. Normally, this information is submitted by the clients, which details the browser, operating system, software vendor or software revision, in an identification string.
%un - Unit Name	Name of the unit, which is same as the default hostname.
%uid - Unique ID	ID generated for the request. A unique ID is generated for every log.
%v - Version	HTTP version used by the request.
%wmf - WF Matched	Specifies whether the request is valid. Values: INVALID, VALID.
%tarc - Epoch/Unix Timestamp	Time is displayed in the Epoch/Unix timestamp format.
%ta - American Standard Format Timestamp	Time is displayed in the American Standard timestamp format.
%cfp - Client Fingerprint	A unique client fingerprint generated for the client sending the request.
%rrs - Request Risk Score	Risk score assigned to the request.
%crs - Client Risk Score	Risk score assigned to the client fingerprint.

Log Field Macros for Event Logs

Event Logs	Description
%t - Timestamp	The time recorded in the following format: "yyyy-mm-dd hh:mm:ss.s" (one or more digits representing a decimal fraction of a second) TZD (time zone designator, which is either Z or +hh:mm or -hh:mm)
%lt - LogType	Type of log: Web Firewall Log, Access Log, or Event Log.
%waas_category - Event Log Categories	Category of the event to which the component belongs. The event types are: • ApplicationHealth • ServerHealth • DDoS • Certificate • DNS • License
%waas_application_id - Application ID	ID of the application.
%waas_message - Event Message	Message displayed for the generated event.

When Web Firewall Logs are exported to the configured log server, the attack IDs are prefixed with 29 in the exported logs. For example, if the attack ID for the "Parameter Name Length Exceeded" attack is 147, the ID in the exported logs is displayed as 29147.