# Qualys Context Extended Detection and Response

## Barracuda WAF

Data Mapping Guide

February 14, 2022

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

# Table of Contents

# About this Guide

Thank you for your interest in Extended Detection, and Response (XDR). Qualys Context XDR expands the capabilities of the Qualys Cloud Platform to integrate data points from other Qualys products offer a unified view of your organization's security posture. Context XDR integrates data points (events/logs) from your enterprise's ecosystem that comprises of several heterogenous sources. This data is normalized, enriched and then categorized before storing it in the Qualys Context XDR data model. This unified database that holds data points from multiple security applications is then used to offer a 360° view of your organization's security posture — all from a single solution.

The Data Mapping Guides provide a list of the fields received through a data source and how these fields are mapped to the Qualys Context XDR data model.

## About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

## Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at http://www.qualys.com/support/.

# Overview

Qualys Extended Detection and Response (XDR) can be configured to ingest data from several different data sources. Each data source has its own data points, and this Data Mapping Guide offers insight into how these data points are interpreted, normalized, and mapped in Qualys Context XDR.

This guide focuses on the data mapping between Barracuda WAF fields and the Qualys data model.

**Note**: For a complete list of sources that Qualys Context XDR supports, on the Qualys Context XDR UI, navigate to **Configuration** > **Data Collection** > **Catalog**. If the source you are looking for is not in the catalog, you can add a request for support using the **Not in the list?** card. Based on the requests coming in, Qualys will prioritize and attempt to add support at the earliest.

## Device Details

- **Device Type** – WAF
- **Device Vendor** – Barracuda
- **Device Product** – Barracuda WAF
- **Supported Versions** – Limited Support – Contact your TAM for further information.

## Supported Formats

In Qualys Context XDR, you can configure to receive data from Barracuda WAF using the following formats:

- **Syslog**

For information on configuring collectors, refer to the Deploying a Collector section in the Online Help.

## Data Field Mappings

This section provides a detailed mapping of the data source fields to the Qualys Context XDR.

**deviceType** – WAF
**deviceVendor** – Barracuda

| Data Source Fields | Qualys Context XDR QQL Tokens | Sample Values | Description |
|---|---|---|---|
| Time | eventTime | 8/31/2020 23:59 | 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) |
| Host | deviceHost | VA-R-BG-WAF1 | Specifies the name of the unit, which is the same as the Default Hostname on the BASIC > IP Configuration page. |
| Vendor | deviceVendor | Barracuda | Vendor name of the device that is producing the audit events |
| Type | deviceType | WAF | Type of the device that is producing the audit events |
| Model | deviceModel | 1010 | Model details of the device that is producing the audit events |
| Severity | deviceSeverity | INFO | Defines the severity of the attack.<br>**Possible values**:<br>• EMERGENCY – System is unusable (highest priority)<br>• ALERT – Response must be taken immediately<br>• CRITICAL – Critical conditions<br>• ERROR – Error conditions<br>• WARNING – Warning conditions<br>• NOTICE – Normal but significant condition<br>• INFORMATION – Informational message (on ACL configuration changes)<br>• DEBUG – Debug-level message (lowest priority)<br>For information Qualys normalized values, click here. |
| src | sourceIpv4 | 192.168.100.10 | The IP address of the client sending the request. Note that an intermediate proxy or gateway may have overwritten the actual source IP of the client with its own. |
| spt | sourcePort | 57860 | The port relevant to the client IP address |
| dst | destinationIpv4 | 192.168.100.10 | The IP address of the service that receives the traffic |
| dpt | destinationPort | 443 | The port relevant to the IP address of the service |
| app | application | Application | Name of the application used. |
| in | inByte | 655 | Traffic in Bytes received by the user as present in the event |

| Data Source Fields | Qualys Context XDR QQL Tokens | Sample Values | Description |
|---|---|---|---|
| out | outByte | 1204 | Traffic in Bytes sent by the user as present in the event |
| requestMethod | method | POST | The request method of the traffic |
| httpStatus | status | 200 | HTTP status codes |
| host | requestUrl | api-tfnregistry.somos.com | The URL specified in the request |
| referer | referrerUrl | - | Referred URL for the RequestURL |
| rt | receivedTime | 1598932795652 | The time at which the log was received by XDR |
| logType | eventType | TR | Specifies the type of log: Web Firewall Log, Access Log, Audit Log, Network Firewall Log, or System Log.<br>**Possible values**: WF, TR, AUDIT, NF, SYS |
| httpVersion | httpVersion | HTTP/1.1 | |
| timeTaken | duration | 34 | Time field. e.g. session duration, scan duration, attack duration |
| userAgent | userAgent | python-requests/2.22.0 | user_agent used to request the URL |
| Proxy IP | additionalIP | 198.143.33.4 | If the client requests are coming through a proxy or gateway, this field provides the IP address of the proxy. A client-side proxy or gateway changes the source IP of the request to its own and embeds the actual client's IP in an HTTP header such as X-Forwarded-For or X-Client-IP. The Barracuda Web Application Firewall, if configured, will ignore the proxy IP and extract the actual client IP from the appropriate header to apply security policies as well as for logging the Client IP field above. This field preserves the proxy IP address for cases where it is required, e.g., forensics and analytics. |
| Attack Type | eventName | MISSING_REFERER_HEADER | The name of the attack triggered by the request |
| Rule | policy | global | The path of the URL ACL that matched with the request. |
| Action | action | LOG | The appropriate action applied on the traffic.<br>**Possible values**:<br>• DENY – denotes that the traffic is denied<br>• LOG – denotes monitoring of the traffic with the assigned rule<br>• WARNING – warns about the traffic<br><br>For information on Qualys normalized values, click here. |
| Follow-up Action | secondaryAction | NONE | The follow-up action as specified by the action policy. It can be either None or Locked in case the lockout is chosen. |

| Data Source Fields | Qualys Context XDR QQL Tokens | Sample Values | Description |
|---|---|---|---|
| Attack Details | detectionMethod | [Referer header is missing] | Details of the attack triggered by the request |
| Attack ID | deviceEventId | - | Event ID assigned by the device which is producing the audit events if present in the audit log |
| UID | externalId | 17447d21893-dc97b899 | Unique ID |
| Authenticated User | sourceUser | Bearer | The username of the currently authenticated client requesting the web page. This is available only when the request is for a service that is using the AAA (Access Control) module. |

## Qualys Internal Fields

| Qualys Context XDR QQL Tokens | Sample Values |
|---|---|
| deviceType | WAF |
| deviceModel | 1010 |
| deviceVendor | Barracuda |
| deviceHost | el.xyz.com |
| customerId | d656b196-edb7-45e6-8485-3748a740d002 |
| collectorId | ae102769-bd05-415d-af3c-2cc59681cbab |
| eventSourceId | 1ae639f0-0944-4cbc-81ef-87c040ca9eb2 |
| eventId | d656b196-edb7-45e6-8485-3748a740d002 |
| collectorReceivedTime | Jun 01, 2021 11:29:04 AM |

## Field Value Mappings

### Data source field: Severity

| Source Values | Qualys Normalized Values |
|---|---|
| Emergency | Emergency |
| ALERT | Alert |
| Critical | Critical |
| Error | Error |
| Warning | Warning |
| Notice | Notice |
| INFO | Informational |
| Debug | Debug |

### Data source field: Action

| Source Values | Qualys Normalized Values |
|---|---|
| DENY | Deny |
| LOG | Log |
| WARNING | Warning |