# Qualys Context Extended Detection and Response

## Citrix Web Application Firewall

Data Mapping Guides

January 22, 2023

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

# Table of Contents

**About this Guide** ..... **4**
About Qualys ..... 4
Qualys Support ..... 4
**Overview** ..... **5**
Device Details ..... 5
Supported Formats ..... 5
**Data Field Mappings** ..... **6**
Qualys Internal Fields ..... 8

# 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 Citrix Web Application Firewall 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** – Citrix
- **Device Product** – Citrix WAF
- **Supported Versions** – Limited Support – Contact your TAM for further information.

## Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Citrix Web Application Firewall using the following formats:

- **JSON**

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** – Web Application Firewall
**deviceVendor** – Citrix

| | | Sample Values | Description |
|---|---|---|---|
| Event Time | eventTime | Sep 15 14:13:51 | Time of the event |
| Host | deviceHost | 192.168.100.10 | Metadata field |
| Description | description | Device supports the following 4 cipher(s) | Rest of the fields from raw message |
| Device Severity | deviceSeverity | 6 | Severity details for the event log as per the device which is producing the audit events |
| Device Event ID | deviceEventId | %FW-6-DROP_PKT | Event ID assigned by the device which is producing the audit events if present in the audit log |
| Event Type | eventType | DROP_PKT | Type of the email Recipient |

| Data Source Fields | Qualys Context XDR QQL Labels | Sample Values | Description |
|---|---|---|---|
| | eventTime | Apr 22 05:50:09 | The time at which the log is generated |
| | deviceHost | lb02.s01.sjc01.qualys.com | - |
| | | CEF:0 | Log format |
| | | Citrix | Vendor name of the device which is producing the audit events |
| | deviceModel | NetScaler | Model name of the device which is producing the audit events |
| | Version | NS13.0 | Version of the device |
| | processName | APPFW | Module Name |

| Data Source Fields | Qualys Context XDR QQL Labels | Sample Values | Description |
|---|---|---|---|
| | eventType | APPFW_FIELDCONSISTENCY | |
| src | sourceIpv4 | 5.196.45.62 | IP of the requested user |
| spt | sourcePort | 47844 | Port of the requested user |
| method | method | GET | Method used to Request the URL. |
| request | requestUrl | https://community.qualys.com/blogs?community\=2001 | URL Requested in the event log |
| msg | message | Field consistency check failed, missing Form-ID | Message regarding the observed security check violation |
| cn1 | deviceEventId | 273809386 | Event ID added by the source to the log |
| cn2 | externalId | 848439458 | HTTP Transaction ID |
| cs1 | object | Qualys_Profile_Learn | Request processed profile name |
| cs2 | | PPE1 | PPE ID |
| cs3 | sessionId | | Application firewall session ID |
| cs4 | deviceSeverity | ALERT | Severity of the event generated.(eg. ALERT, INFO) |
| cs5 | | 2021 | Year in which the event generated |
| cs6 | category | web-cgi | Signature Violation Category |
| act | action | not blocked | The action taken by application firewall. Possible values are blocked, not blocked, transformed |

## Qualys Internal Fields

| Qualys Context XDR QQL Tokens | Sample Values |
|---|---|
| DeviceType | WAF |
| DeviceModel | NetScaler |
| DeviceVendor | Citrix |
| DeviceHost | - |
| 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 |