



# **Qualys Context XDR (Extended Detection and Response)**

## **VMware Application**

Data Mapping Guide

April 21, 2022

Copyright 2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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

## Table of Contents

|                                  |          |
|----------------------------------|----------|
| <b>About this Guide</b> .....    | <b>4</b> |
| About Qualys.....                | 4        |
| Qualys Support .....             | 4        |
| <b>Overview</b> .....            | <b>5</b> |
| Device Details.....              | 5        |
| Supported Formats .....          | 5        |
| <b>Data Field Mappings</b> ..... | <b>6</b> |
| Qualys Internal Fields .....     | 7        |

## 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 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](http://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 Context 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 VMware Application fields and the Qualys data model.

**Note:** For a complete list of sources that Qualys XDR supports, on the Qualys 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** – Application
- **Device Vendor** – VMware
- **Device Product** – VMware Application
- **Supported Versions** – 6.5, 6.7, 7.0

## Supported Formats

In Qualys Context XDR, you can configure to receive data from VMware Application 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** – Application

**deviceVendor** – VMware

| Data Source Fields | Qualys Context XDR QQL Tokens | Sample Values   |
|--------------------|-------------------------------|---|
| Log time           | eventTime                     | 2021-07-23T10:02:51Z  |
| Process            | processName                   | sshd  |
| Process ID         | processId                     | 7828034   |
| Message            | eventName                     | PAM: User not known to the underlying authentication module |
| Source             | sourceIpv4                    | 10.44.26.53s  |
| Source Port        | sourcePort                    | 53648   |
| Source User        | sourceUser                    | admin   |
| Source Host        | sourceHost                    | 10.44.26.54   |
| Module             | object                        | pam_unix(sshd:auth)   |
| Tally              | count                         | 6   |
| Denied Count       | accessDenied                  | 5   |
| Outcome            | outcome                       | Failure   |
| Application        | application                   | ssh2  |

## Qualys Internal Fields

| Qualys Context XDR<br>QQL Tokens | Sample Values                        |
|----------------------------------|--------------------------------------|
| customerId                       | 2104c860-925a-4572-9ae6-e4c9c6b8fdab |
| deviceType                       | Application                          |
| deviceModel                      | ESXi                                 |
| deviceVendor                     | VMware                               |
| deviceHost                       | -                                    |
| collectorId                      | e22ca2cf-26db-4974-b226-d155f22ebfc6 |
| eventSourceId                    | 69608d8a-4088-4c6d-be0c-f3d5108f25d6 |
| eventId                          | c664ac73-0e9b-46d8-98f0-bf0dae79ae09 |
| collectorReceivedTime            | Sep 14, 2021 11:29:04 AM             |