Qualys Context Extended Detection and Response

Juniper Pulse Secure VPN

Data Mapping Guide

February 18, 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 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 Juniper Pulse Secure VPN 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** – VPN
- **Device Vendor** – Juniper
- **Device Product** – Juniper Pulse Secure
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from Juniper Pulse Secure VPN using the following formats:

-

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 – VPN
deviceVendor – Juniper

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
id	recordType	firewall	The type of record. For log files conforming to this document, the type will always be firewall.
time	eventTime	2020-02-11 08:09:26	The date and time of the event, in terms of local time
pri	pulsePriority	2	The priority of the event
fw	deviceIPAddress	192.168.100.10	The firewall that generated the log record. This is most often represented as an IP address or a machine name.
vpn	object	ive	Identifies a particular VPN. This value is used to generate tables showing the most highly used VPNs and tables correlating particular users to particular VPNs.
user	sourceUser	System	The authenticated user name, if users are authenticating through the firewall
realm	userRealm	COWES - 2FA	Specifies the conditions that users must meet to sign into the system. A realm consists of a grouping of authentication resources.
roles	userRole	Portal_Cowes GENERAL (CWSRDS), Portal_Cisco, Portal_Poland	Entity that defines user session parameters (session settings and options), personalization settings (user interface customization and bookmarks), and enabled access features (Web, file, secure application manager, VPN tunneling, Secure Email, enterprise onboarding Telnet/SSH, Terminal Services, meeting, e-mail access, virtual desktops, HTML5 access, and Pulse Secure client)
type	vpnType	mgmt	The firewall vendor can use the type= field to cause records to be placed into the tables relating to VPN events or relating to firewall management events.
proto	protocol	https, http, ftp, ssh, smb	The protocol used by the event
src	sourceIpv4	192.168.100.10	The IP address that generated the event
dst	destinationIpv4	192.168.100.10	The IP address that received the event.
dstname	destinationHost	logsvr1.filton.cisco.local	A more user-friendly version of the dst= field
sent	outByte	13449, 300, 5846	The number of bytes transferred from the source to the destination
rcvd	inByte	368371, 300, 4951	The number of bytes transferred from the destination to the source

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
msg	message	NTP server '10.231.16.127' is unreachable or the symmetric key provided is incorrect.	Basis for the tables showing detailed Critical Events, Errors and Warnings, VPN events, and Firewall Management events.
Derived Fields	deviceEventId	ADM20652	Event ID assigned by the device that is producing the audit events if present in the audit log
Derived Fields	eventType	SystemError	Type of the event
Derived Fields	eventSubType	Misc	SubType of the event associated with the EventType field
Derived Fields	severity	Critical	XDR severity assigned to this log audit
Derived Fields	eventName	NTP Server Unreachable	A brief standard meaning of the message that makes it easy to read
Reason	reason	sslv3 alert certificate unknown	Connection status details
File Size	fileSize	80257333	Size of the archived file
Time Taken	duration	59	Duration to archive the file

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	VPN
deviceModel	Pulsesecure
deviceVendor	Juniper
deviceHost	DC2-PA-XXX.npi.int
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