Qualys Context Extended Detection and Response

Citrix 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 Citrix VPN 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** – VPN
- **Device Vendor** – Citrix
- **Device Product** – Citrix VPN
- **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 VPN 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 – VPN
deviceVendor – Citrix

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
Event Time	eventTime	13/08/2019:13:49:11	The time at which the event occurred
Device	deviceName	XenAGEE	The device on which the session was logged
Message	eventName	ICAEND_CONNSTAT, LOGIN_FAILED	Log format for the Syslog Message Reference
Severity	deviceSeverity	0	Severity associated with the event
Source	sourceIpv4	10.200.244.37	Original session source IP address
Destination	destinationIpv4	10.0.96.25	Original session destination IP address
Source Port	sourcePort	60154	Original session source IP port
Destination Port	destinationPort	2598	Original session destination IP port
Nat_ip	natSourceIP	36.255.31.246	Original NAT IP
Total_bytes_recv	inByte	3345996	Number of bytes in the server-to-client direction of the session
Total_bytes_send	outByte	209801	Number of bytes in the client-to-server direction of the session
Vserver	virtualSystem	36.255.31.246	Virtual Server IP
Vserver Port	virtualPort	443	Port of the virtual server
startTime	beginningTime	08/13/2019:14:11:24	Time the log was sent at the management plane
endTime	endTime	08/13/2019:14:16:31	Time the log was received at the management plane
Duration	duration	00:05:07	The elapsed time of the session
PPE	packetEngine	PPE	The packet engine is created to perform TCP/IP processing, and is responsible for all load balancing acceleration
PPE Id	ppeId	1	ID of the packet processing engine
Count	count	2	Count of the number of sessions
Category	category	AAA	IP protocol associated with the session
Log Format	logFormat	0	Log format of the syslog message
connectionId	externalId	9b642657	A unique identifier of a connection established
VPN Session	sessionId	3219635502	Unique number given to every log
Browser	userAgent	CitrixReceiver/com.zenprise build/1.0 Android/7.1.1 NMF26X.T355YDOU1CRB3 VpnCapable X1Class	User-Agent that facilitates end user connection
Status	outcome	success	Status of the request

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
URL	requestUrl	akamai.com	The domain which the user is connecting to
User	userName	anonymous	User being authenticated
Group(s)	group	N/A	Group Name
Failure_reason	message	External authentication server denied access	Failure reason due to which the server was denied access
Internal Fields	tags	VPN	Different tags for more details like device type, jdbc, parser details
applicationName	application		Name of application
Internal Fields	eventContext	local-to-remote, remote-to-local	Context of Connection: Ingoing / Outgoing
Internal Fields	userEmployeeId	QS100302	Unique ID to identify an employee
Internal Fields	userDepartment	Engineering	Department of employee
Internal Fields	userStatus	Full Time Employee	

Qualys Internal Fields

Qualys Context XDR QQL Tokens	**Sample Values**
DeviceType	VPN
DeviceModel	NetScaler Gateway
DeviceVendor	Citrix
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	Sep 14, 2021 11:29:04 AM
geoSourceCoordinates	37.3526,-121.9541
geoDestinationCoordinates	34.164,-118.2387
geoSourceCountry	United States, India
geoDestinationCountry	United States, United Kingdom
geoSourceCity	Santa Clara, Kolkata
geoDestinationCity	Glendale, New York

Field Value Mappings

Data source field: VPN

Source Values	**Qualys Normalized Values**
success	Success
failure	Failure