Qualys Context Extended Detection and Response

Fortinet Firewall

Data Mapping Guide

February 18, 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

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 Fortinet 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** – Firewall
- **Device Vendor** – Fortinet
- **Device Product** – Fortinet Firewall
- **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 Fortinet Firewall using the following format:

- **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 data model.

deviceType – Firewall
deviceModel – FortiGate
deviceVendor - Fortinet

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
date	receivedTime	2020-11-19	Data source field “date” and “time” are combined and mapped to *receivedTime*. *date* - Day, month and year when the log message was recorded *time* - Hour clock when the log message was recorded
time		13:02:56	
duration	duration	225	Duration of the session
sessionid	sessionId	77324595	ID for the session
vd	virtualDomain	root	Name of the virtual domain in which the log message was recorded
transport	natSourcePort	49192	NAT source port
srcip	sourceIpv4	10.0.13.168	IP address of the traffic’s origin - HTTP requests - web browser or other client - HTTP responses - physical server
srcport	sourcePort	49393	Port number of the traffic's origin
srcintf	sourceInterface	CS-To-AWS2	Interface name of the traffic's origin
transip	natSourceIP	0.0.0.0	NAT source IP
srccountry	geoSourceCountry	Reserved	Source country name
srcname	sourceHost	pc1	Source name
osname	osDetails	Linux	Source OS
srcmac	sourceMac	a2:e9:00:ec:40:01	MAC address associated with the source IP address
dstmac	destinationMac		MAC address associated with the destination IP address
devid	deviceId	FG200D3915802513	Device serial number for the traffic's origin
devname	deviceName	Primary_Fortigate	Hostname of the device where event is produced/logged
dstip	destinationIpv4	172.168.1.1	Destination IP address for the web
dstport	destinationPort	53	Traffic destination’s port number
tranip	natDestinationIP		NAT destination IP
dstintf	destinationInterface	port2	Traffic destination’s interface

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
dstcountry	geoDestinationCountry	Reserved	Destination country
dstname	destinationHost	fortiguard.com	Destination name
app	application	HTTPS.BROWSER	Application name
service	sourceServiceName	DNS	Service name
appcat	applicationCategory	unscanned	Application category
apprisk	applicationRiskLevel	medium	Application risk level
sentbyte	outByte	360	Number of bytes sent
rcvdbyte	inByte	360	Number of bytes received
sentpkt	packetsOut	8	Number of packets sent
rcvdpkt	packetsIn	8	Number of packets received
action	action	accept	Session status. Uses following definitions: - **Deny**: blocked by firewall policy - **Start**: session startlog (special option to enable logging at start of a session). This means firewall allowed. - **All Others**: allowed by Firewall Policy and the status indicates how it was closed For information on how each individual value is mapped in Qualys, click here.
policytype	policy	policy	policyname/rulename from the device
level	deviceSeverity	notice	Security level rating For information on how each individual value is mapped in Qualys, click here.
eventtime	eventTime	1605808976	Epoch time the log was triggered by FortiGate. If you convert the epoch time to human readable time, it might not match the Date and Time in the header owing to a small delay between the time the log was triggered and recorded. The Log Time field is the same for the same log among all log devices, but the Date and Time might differ.
proto	protocol	17	Protocol used by web traffic (By default, TCP)
type	eventType	traffic	Log type: Anomaly, App, AV, CIFS, DLP, DNS, Email, Event, GTP, IPS, SSH, SSL, Traffic, VoIP, WAF, Web Filtering
logid	deviceEventId	0000000020	A unique 10-digit identifier for a log and includes the information about the log entry. For more information on the logid, refer these links: • Log ID definitions • Log ID numbers

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
subtype	eventSubType	forward	Represented by the second two digits of the log ID. In event logs, some of the subtypes are compliance check, system, and user. In traffic logs, the subtypes are forward, local, multicast, and sniffer. For more information on the subtype, refer these links: • Subtype • List of log types and subtypes
utmaction	secondaryAction	allow	Security action performed by UTM. For information on how each individual value is mapped in Qualys, click here.
vpn	vpnTunnelName	CS-To-AWS2	VPN tunnel name
user	sourceUser	hkumar	Username
logdesc	reason	Outdated report files deleted	Log description
msg	message	Delete 4 old report files	
Crlevel	clientReputationLevel	low	Client Reputation level
eventtype	webFilterEventType	app-ctrl-all	Web Filter event type
hostname	requestUrl	images.attackiq.com	The hostname of a URL
incidentserialno	externalId	1796479584	Associated ID given in the event by the event source.
direction	direction	outgoing	Direction
group	group	N/A	User Name Group
Role	firewallRole	initiator	Role
version	version	3.502516	Application version/device version present in the log
result	outcome	OK	For information on how each individual value is mapped in Qualys, click here.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Firewall
deviceModel	FortiGate
deviceVendor	Fortinet
deviceHost	10.10.x.x
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
eventName	Traffic logs, Event logs

Field Value Mappings

Data source field: level

Source Values	Qualys Normalized Values
emergency	Emergency
alert	Alert
critical	Critical
error	Error
warning	Warning
notice	Notice
information	Information

Data source field: action/utmaction

Source Values	Qualys Normalized Values
deny	Deny
accept	Allow
start	Start
dns	DNS
ip-conn	IP-conn
negotiate	Negotiate
block	Block
install_sa	Install_sa
pass	Pass
close	Close
timeout	Timeout
client-rst	Reset-Client
server-rst	Reset-Server

Data source field: result

Source Values	Qualys Normalized Values
OK	Ok
DONE	Done