Qualys Context Extended Detection and Response

HP Aruba Wireless Network Device

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 HP Aruba Wireless Network Device 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** – Wireless Network Device
- **Device Vendor** – HP
- **Device Product** – HP Aruba Wireless Network Device
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from HP Aruba Wireless Network Device 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 – Wireless Network Device
deviceVendor – HP

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
username	sourceUser	mallory.spencer	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)
userip	sourceIpv4	0.0.0.0	IPv4 address of the source machine (the machine that has generated this event as per the log audit)
usermac	sourceMac	9c:2a:70:0e:35:11	MAC address of the source machine (the machine that has generated this event as per the log audit)
servername	wirelessServerName	cppm-3	RADIUS server for authentication
serverip	wirelessServerIp	153.90.2.250	
apname	destinationHost	2155AP127-1	Access Point name
bssid	destinationMac	4:bd:88:70:96:e1	Access Point bssid
msg	eventName	WPA2 Key Message 2	A brief standard meaning of the message that is easy to read
prof	wirelessProfileValue		
stcnt	stationCount	1	
apcnt	accessPointCount	3	
ssid	wirelessSsid	MSU-Secure	
AAA profile	wirelessAaaProfile	MSU_Secure_Clearpass-aaa_prof	
sin_port	radiusServerPort	1812	
eventID	deviceEventId	522275	A unique number within the set of messages generated by Aruba OS
category	eventType	User messages	Message category
EventTime	eventTime	2021-02-26T05:49:45+00:00	Timestamp showing when the message was created
processDescription	eventSubType	User authentication	Controller process description. For example, the authmgr process is for User authentication. For all possible values, refer this table.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
subcat	category	aaa, all, dot1x, firewall, ike, mobility, packet-trace, vpn, webserver	Message subcategory, which depends upon the message category specified.
severity	deviceSeverity	ERRS	Message severity level
processName	processName	authmgr	Controller process
processId	processId	4132	Unique process ID
action	action	0x8001	Action taken in the event log

EventSubType Values

Process Name	Description
aaa	AAA logging
ads	Anomaly detection
approc	AP processes
authmgr	User authentication
cfgm	Configuration Manager
crypto	VPN (IKE/IPsec)
cts	Transport service
dbsync	Database synchronization
dhcpd	DHCP packets
esi	External Services Interface
fpapps	Layer 2 and 3 control
httpd	Apache
l2tp	L2TP
licensemgr	License manager
localdb	Local database
mobileip	Mobile IP
packetfilter	Packet filtering of messaging and control frames
phonehome	PhoneHome
pim	Protocol Independent Multicast
pppoed	PPPoE
pptp	PPTP
processes	Run-time processes
profmgr	Profile Manager
publisher	Publish subscribe service
rfm	RF Troubleshooting Manager
snmp	SNMP
stm	Station management
syslogdwrap	Syslogd wrap
traffic	Traffic
vrrpd	VRRP
wms	Wireless management (master controller only)

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Wireless Network Device
deviceModel	Aruba
deviceVendor	HP
deviceHost	MSU_7220_Local2
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

Field Value Mappings

Data source field: Severity

Source Values	Qualys Normalized Values
EMERG	Emergency
ALERT	Alert
CRIT	Critical
ERRS	Error
WARN	Warning
NOTI	Notice
INFO	Informational
DEBUG	Debug