Qualys Context Extended Detection and Response

McAfee Web Gateway Proxy

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 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 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 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 XDR.

This guide focuses on the data mapping between McAfee Web Gateway Proxy 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** – Proxy
- **Device Vendor** – McAfee
- **Device Product** – McAfee Web Gateway Proxy
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Formats

In Qualys XDR, you can configure to receive data from McAfee Web Gateway Proxy 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 XDR.

deviceType – Proxy
deviceVendor – McAfee

Data Source Fields	Qualys XDR QQL Tokens	Sample Values	Description
Timestamp	receivedTime	01-07-2013 08:47	Time when logs was received
Device Name	deviceName	TCX-PROXY-1B	Hostname of the device where event is produced/logged
LEEF Version	leefVersion	1	Version for the Log Event Extended Format
Device Vendor	deviceVendor	McAfee	Vendor name of the device which is producing the audit events
Device Model	deviceModel	Webgateway	Model details of the device which is producing the audit events
Device Version	version	7	Application/device version present in the log
Error Code	errorCode	81	
Event Name	eventName	Proxy logs	Brief standard meaning of the message
devTime	eventTime	1.59466E+12	Time of the event
src	sourceIpv4	10.61.241.158	IPv4 address of the source machine (the machine that has generated this event as per the log audit)
usrName	sourceUser		Username present in the log apart from source and destination username
httpStatus	status	407	HTTP status codes
dst	destinationIpv4	172.232.11.170	IPv4 address of the destination machine (the machine that has generated this event as per the log audit)
urlCategories	objectCategory	Business, Software/Hardware	URL categorization of the URL in event log. (Primarily used for URL categorization)
blockReason	reason	Authentication Required	Connection status details
url	requestUrl	https://statics.teams.cdn.office.net	URL Requested in the event log
host	destinationHost	statics.teams.cdn.office.net	Hostname of the destination machine (the machine towards which this event is directed as per the log audit)
bytes_from_client	inByte	403	Traffic in Bytes received by the user as present in the event
bytes_from_server	outByte	100695	Traffic in Bytes sent by the user as present in the event

Data Source Fields	Qualys XDR QQL Tokens	Sample Values	Description
user_agent	userAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Teams/1.3.00.13565 Chrome/69.0.3497.128 Electron/4.2.12 Safari/537.36	user_agent used to request the URL
virus_name	risk		Virus name or the detection name from the event
hash	md5Hash		MD5 hash value of the file
filename	fileName		File name as present in the audit event
filesize	fileSize	0	File size as present in the audit event
content-length	contentLength	0	
Source Geo Coordinates	geoSourceCoordinates	Geo Co-ordinates of Source IP	Geo coordinates of the source IP for the audit log. Can be part of enrichment
Destination Geo Coordinates	geoDestinationCoordinates	Geo Co-ordinates of Destination IP	Geo coordinates of the destination IP for the audit log. Can be part of enrichment
Source Geo Country	geoSourceCountry	Source IP location by country	Country name of the source IP for the audit log. Can be part of enrichment
Destination Geo Country	geoDestinationCountry	Destination IP location by country	Country name of the destination IP for the audit log. Can be part of enrichment
Source Geo City	geoSourceCity	Source IP location by city	City name of the source IP for the audit log. Can be part of enrichment
Destination Geo City	geoDestinationCity	Destination IP location by city	City name of the destination IP for the audit log. Can be part of enrichment
Event Context	eventContext		Event Context, remote-to-local, local-to-local, local-to-remote

Qualys Internal Fields

Qualys XDR QQL Tokens	Sample Values
deviceType	Proxy
deviceModel	Webgateway
deviceVendor	McAfee
deviceHost	
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