Qualys Context Extended Detection and Response

Cisco AnyConnect VPN

Data Mapping Guide

February 16, 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 Cisco AnyConnect 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** – Cisco
- **Device Product** – Cisco AnyConnect
- **Supported Versions** – 9.12(2)5

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Cisco AnyConnect 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 – Cisco

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Event ID	deviceEventId	%ASA-6-113005	Event ID assigned by the device which is producing the audit events if present in the audit log
Host	deviceHost	IE11Win7	Metadata field
Device Severity	deviceSeverity	6	Severity details for the event log as per the device which is producing the audit events
Timestamp	eventTime	Nov 03 2020 09:50:01	Time of the event
Event Name	eventName	AAA user authentication Rejected	Brief standard meaning of the message easy to read for Analyst
reason	reason	AAA failure	Connection status details
server/dst-ip	destinationIpv4	192.168.100.10	IPv4 address of the destination machine (the machine who has generated this event as per the log audit)
domain_name	sourceDomain	LOCAL	Domain name of the source machine (the machine who has generated this event as per the log audit)
Interface	sourceInterface	outside	Interface name on the source machine (the machine who has generated this event as per the log audit)
src-port	sourcePort	50188	Natted port on the source machine (the machine who has generated this event as per the log audit)
dst-port	destinationPort	443	Port used on the destination machine (the machine who has generated this event as per the log audit)
protocol	protocol	TLSv1.2	Protocol used in the event log
action	action	terminated	Action taken in the event log
user IP/IP/IPv4 Address	sourceIpv4	192.168.100.10	IPv4 address of the source machine (the machine who has generated this event as per the log audit)
Policy	policy	Group being set to Dev	Policyname/rulename from the device
Group	group	Dev	Group Name to which entity(asset/user) in audit log belong
SVC Message	vpnClientMessage	16	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
IPv6 address	sourceIpv6	FE80:0000:0000:0000:0202:B3FF:FE1E:8329	IPv6 address of the source machine (the machine who has generated this event as per the log audit)
Session	sessionId	0x00925000	Session id from the event log
user	sourceUser	john.doe	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)
IP	natSourceIP	192.168.100.10	Natted IP address of the source machine (the machine who has generated this event as per the log audit)
Event Type	eventType	SVC connection	Type of the event. (E.g. TRAFFIC, SYSTEM)
Outcome	outcome	Failure	Outcome of the event

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	VPN
deviceModel	AnyConnect
deviceVendor	Cisco AnyConnect
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	Jun 01, 2021 11:29:04 AM

Field Value Mappings

Data source field: severity

Source Values	Qualys Normalized Values
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug

Data source field: action

Source Values	Qualys Normalized Values
Built	Allow
Teardown	Block
Deny	Deny
denied	Deny
requested	Request
permitted	Allow
Denied	Deny
denied by ACL	Deny
discarded	Discarded
est-allowed	Allow
Dropping	Drop
created	Created
deleted	Deleted