Qualys Context XDR (Extended Detection and Response)

Cisco ASA Firewall

Data Mapping Guide

March 24, 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 XDR (Extended Detection and Response) 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 ASA 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** – Cisco
- **Device Product** – Cisco ASA Firewall
- **Supported Versions** – 7.0, 9.8

Supported Collectors

In Qualys Context XDR, you can configure to receive data from Cisco ASA Firewall using the following collectors:

- **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 – Firewall
deviceVendor – Cisco-ASA

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Event Time	eventTime	Sep 15 14:13:51	Time of the event
Host	deviceHost	192.168.100.10	Metadata field
cause	reason	User was not found	Connection status details
Direction	direction	inbound	Direction of the traffic or event
Protocol	protocol	icmp	Protocol used in the event log
Action	action	Deny	Action taken in the event log
IP_address	sourceIpv4	192.168.100.10	IPv4 address of the source machine (the machine who has generated this event as per the log audit)
port	sourcePort	50002	Port used on the source machine (the machine who has generated this event as per the log audit)
IP_address	destinationIpv4	192.168.100.10	IPv4 address of the destination machine (the machine who has generated this event as per the log audit)
port	destinationPort	2218	Port used on the destination machine (the machine who has generated this event as per the log audit)
Flags	customString12	SYN ACK	
idfw_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)
idfw_user	destinationUser	kjohn	Username using/logged-in the destination machine (the username present in the log audit as per the log audit logged by the device)
src interface_name	sourceInterface	outside	Interface name on the source machine (the machine who has generated this event as per the log audit)

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
dst interface_name	destinationInterface	inside	Interface name on the destination machine (the machine who has generated this event as per the log audit)
connections	count	76484	Total count of the event logs incase they are aggregated
time	duration	0:00:10	Time field. e.g. session duration, scan duration, attack duration
url	customString13	http://tile-service.weather.microsoft.com/en-US/livetile/preinstall?region=PH&appid=C98EA5B0842DBB9405BBF071E1DA76512D21FE36&FORM=Threshold	
connections	customString10	5538	
acl-name	sourceHost	IE11Win7	Hostname of the source machine (the machine who has generated this event as per the log audit)
real_address	destinationHost	IE11Win7	Hostname of the destination machine(the machine towards which this event is directed as per the log audit)
mapped_address	natSourceIP	192.168.100.10	Natted IP address of the source machine (the machine who has generated this event as per the log audit)
mapped_port	natSourcePort	25	Natted port on the source machine (the machine who has generated this event as per the log audit)
bytes	totalBytes	8618	Total Bytes value as present in the event
idfw_user	userName	Mercilla.spencer	userName
interface_name	customString6	outside	
seq_num	externalId	0x317C28	Associated ID given in the event by the event source.
Description	description	Device supports the following 4 cipher(s)	Rest of the fields from raw message

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Outcome	outcome	Failure	Outcome of the event
Group	group	192.168.100.10	Group Name to which entity(asset/user) in audit log belong
Object	customString11	Scanning	
Burst Rate Value	customNumber1	1	
Max Burst value	customNumber2	8	
Average Rate Value	customNumber3	21	
Max Average Value	customNumber4	4	
Service	customString7	ssh	
cmd	command	username admintest password * privilege	This filed captures the 'command' used in the audit log
Bytes xmt	outByte	850	Traffic in Bytes sent by the user as present in the event
Bytes rcv	inByte	98	Traffic in Bytes received by the user as present in the event
Event Name	eventName	Deny Inbound UDP due to DNS Query	brief standard meaning of the message easy to read for Analyst
mapped_address	natDestinationIP	192.168.100.10	Natted IP address of the destination machine(the machine who has generated this event as per the log audit)
mapped_port	natDestinationPort	2346	Natted port on the destination machine(the machine who has generated this event as per the log audit)
service	destinationServiceName	ssh	Service name on the destination machine(the machine who has generated this event as per the log audit)
file	fileName		File name as present in the audit event
Device Severity	deviceSeverity	2	Severity details for the event log as per the device which is producing the audit events

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Device Event ID	deviceEventId	%ASA-2-106001	Event ID assigned by the device which is producing the audit events if present in the audit log
Event Type	eventType	User Authentication	Type of the email Recipient
Event Subtype	eventSubType	Traffic Denied	SubType of the event associated with EventType field.
application-name	application	N/A	name of the application used

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Firewall
deviceModel	ASA
deviceVendor	Cisco
deviceHost	10.220.40.1
customerId	2104c860-925a-4572-9ae6-e4c9c6b8fdab
collectorId	e22ca2cf-26db-4974-b226-d155f22ebfc6
eventSourceId	69608d8a-4088-4c6d-be0c-f3d5108f25d6
eventId	c664ac73-0e9b-46d8-98f0-bf0dae79ae09
collectorReceivedTime	Sep 14, 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