Qualys Context Extended Detection and Response

Juniper Firewall

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 Juniper Firewall 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** – Firewall
- **Device Vendor** – Juniper
- **Device Product** – Juniper 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 Juniper 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.

deviceType – Firewall
deviceVendor – Juniper

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
Event Type	eventType	RT_FLOW_SESSION_CREATE	Type of the event
reason	reason	idle Timeout	Connection Status details
source-address	sourceIpv4	192.168.100.10	The source IP address from where the event occurred
source-port	sourcePort	49847	The source port of the event
destination-address	destinationIpv4	192.168.100.10	The destination IP address of the event
destination-port	destinationPort	389	Destination port of the event
service-name	serviceName	None	The name of the application service. For example, FTP, HTTP, SSH, and so on.
nat-source-address	natSourceIP	192.168.100.10	The translated (or natted) source IP address. It can contain IPv4 or IPv6 addresses.
nat-source-port	natSourcePort	49847	The translated source port
nat-destination-address	natDestinationIP	192.168.100.10	The translated (also called natted) destination IP address
nat-destination-port	natDestinationPort	389	The translated destination port
Protocol-ID	protocol	17	The protocol ID in the log
source-zone-name	sourceZone	corpwan	User traffic received from the zone
destination-zone-name	destinationZone	core	The destination zone of the log
Bytes From Client	outByte	234	Traffic in Bytes sent by the user as present in the event
Bytes From Server	inByte	206	Traffic in Bytes received by the user as present in the event
Elapsed Time	duration	60	Time field. For example, session duration, scan duration, attack duration.
Process Name	processName	sshd, consul, docker-compose, vault	Process name, if present in the event log
Process ID	processId	22645, 54985	Process ID, if present in the event log
Device Name	deviceName	junos@2636.X.X.X.X.35	The host name in the log
Packets From Client	packetsOut	1	Number of packets sent by the user as present in the event
Packets From	packetsIn	1	Number of packets received by the user as

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
Server			present in the event
Device Severity	deviceSeverity	6	Severity details for the event log as per the device which is producing the audit events

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Firewall
deviceModel	OpenDNS, Sourcefire
deviceVendor	Juniper
deviceHost	IAF-Corp-P
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
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notice
6	Informational
7	Debug