Qualys Context Extended Detection and Response

Cisco Identity Services Engine (ISE) IAM

Data Mapping Guide

February 17, 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 Identity Services Engine (ISE) IAM 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** – IAM
- **Device Vendor** – Cisco
- **Device Product** – Cisco ISE
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from Cisco ISE IAM 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 – IAM
deviceVendor – Cisco

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
eventdate	beginningTime	Apr 15 13:49:25	Event/session start time
host	deviceHost	sjc01-soc.cisco.com	Metadata field
category	eventType	CISE_Administrative_and_Operational_Audit	Type of the event. For example, TRAFFIC, SYSTEM
msgId	baseEventId	0000013025	External ID given in the event by the event source.
messageCode	deviceEventId	60080	Message code as defined in the logging categories
level	deviceSeverity	NOTICE	Message severity level of a log message
OperationMessageText	message	2509666 Connection established (TLS)	
AdminName	iseAdminName	admin	
ObjectName	object	System Statistics	Group/policy/registry/domain change
OperationCounters	count	Counter	Total count of the event logs in case they are aggregated
Device IP Address	sourceIpv4	10.250.64.82	IPv4 address of the source machine (the machine that has generated this event as per the log audit)
Device Port	sourcePort	54425	Port used on the source machine (the machine that has generated this event as per the log audit)
DestinationIPAddress	destinationIpv4	10.231.44.61	IPv4 address of the destination machine (the machine that has generated this event as per the log audit)
DestinationPort	destinationPort	1813	Port used on the destination machine (the machine that has generated this event as per the log audit)
Protocol	protocol	Radius	Protocol used in the event log
NetworkDeviceName	deviceName	GBFLTVPN002	Hostname of the device where event is produced/logged
User-Name	sourceUser	ZS88047@CISCO.LOCAL	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)
Framed-Protocol	transportProtocol	PPP	Protocol used to make/facilitate the request as present in the audit log

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Proxy-State	iseProxyState	fe:80:00:00:00:00:00:00:c1:de:1b:59:ec:38:d4:2d:00:02:f4:e3	
AcsSessionID	sessionId	GBCWSISE002/401232868/3416881	Session ID from the event log
FailureReason	reason	RADIUS Accounting-Request header contains invalid Authenticator field	Connection status details
AD-Domain	sourceDomain	cowes.cico.local	Domain name of the source machine (the machine that has generated this event as per the log audit)
SSID	iseSsid	78-72-5d-3d-97-80:p10vnkg	
SelectedAuthorizationProfiles	action	PermitAccess	Action taken in the event log
ConnectionStatus	outcome	Succeeded	Outcome of the event
Software Version	version	8.2.166.0	Application/device version present in the log

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values	Description
deviceType	IAM	Type of the device producing the audit events
deviceModel	ISE	Model details of the device producing the audit events
deviceVendor	Cisco	Vendor name of the device producing the audit events
deviceHost	sjc01-soc.cisco.com	
customerId	d656b196-edb7-45e6-8485-3748a740d002	Unique customer ID
collectorId	ae102769-bd05-415d-af3c-2cc59681cbab	Unique collector ID
eventSourceId	1ae639f0-0944-4cbc-81ef-87c040ca9eb2	Unique event source ID
eventId	d656b196-edb7-45e6-8485-3748a740d002	Unique event ID assigned by Qualys Context XDR
collectorReceivedTime	Jun 01, 2021 11:29:04 AM	Collector Received Time

Field Value Mappings

Data source field: deviceSeverity

Source Values	Qualys Normalized Values
FATAL	Emergency
CRITICAL	Critical
ERROR	Error
WARN	Warning
INFO	Informational
DEBUG	Debug
NOTICE	Notice
UNKNOWN	Unknown

Data source field: outcome

Source Values	Qualys Normalized Values
Succeeded	Success

Data source field: action

Source Values	Qualys Normalized Values
PermitAccess	Allow
DenyAccess	Deny