Qualys Context Extended Detection and Response

Okta IAM

Data Mapping Guide

February 18, 2022

Copyright 2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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 Okta 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** – Okta
- **Device Product** – Okta Application
- **Supported Versions** – 3.5.9

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Okta IAM using the following formats:

- **Splunk**

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 – Okta

Object Type	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
actor	id	sourceUserId	00u14p86tnMKQEQPBLNJ	ID of actor
actor	type	actorType	User	Type of actor – User or SystemPrincipal
actor	alternateId	sourceUser	abc@company.com	Alternative ID of actor
userAgent	rawUserAgent	userAgent	Okta AD Agent/3.5.9 (Microsoft Windows NT 6.2.9200.0; .NET CLR 4.0.30319.42000; 64-bit OS; 64-bit Process; sslpinning=disabled)	A raw string representation of the user agent, formatted according to section 5.5.3 of HTTP/1.1 Semantics and Content. Both the browser and the OS fields can be derived from this field.
userAgent	os	osDetails	Windows 8	Operating system the client runs on (for example, Windows 10)
userAgent	browser	userAgentName	UNKNOWN	If the client is a web browser, this field identifies the type of web browser (for example, CHROME, FIREFOX)
client	zone	sourceZone	null	The name of the zone that the client's location is mapped to
client	id	externalId	cappT0Hfy97F1BoO1UTR	For OAuth requests, this is the ID of the OAuth client making the request. For SSWS token requests, this is the ID of the agent making the request.
client	ipAddress	sourceIpv4	64.39.96.133	IP address that the client made its request from
geographicalContext	city	geoSourceCity	Pune	The city encompassing the area containing the geolocation coordinates, if available (for example, Seattle, San Francisco)
geographicalContext	country	geoSourceCountry	India	Full name of the country encompassing the area containing the geolocation coordinates (for example, France, Uganda)

Object Type	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
attribute.client.geographicalContext.geolocation	geolocation	geoSourceCoordinates		Contains the geolocation coordinates (latitude, longitude)
authenticationContext	externalSessionId	sessionId	trsMknmclJeQiqeu32k58vWhg	A proxy for the actor's session ID
Attribute	displayMessage	eventName	Authenticate user with AD agent	The display message for an event
Attribute	eventType	eventType	user.authentication.auth_via_AD_agent	Type of event that was published
outcome	result	outcome	SUCCESS	Result of the action **Possible values**: SUCCESS, FAILURE, SKIPPED, ALLOW, DENY, CHALLENGE, UNKNOWN Click here for Qualys normalized values.
outcome	reason	reason	null	Reason for the result, for example INVALID_CREDENTIALS
attribute	published	eventTime	2020-09-10T05:23:41.929Z	Timestamp when event was published
attribute	severity	deviceSeverity	INFO	Indicates how severe the event is **Possible values**: DEBUG, INFO, WARN, ERROR Click here for Qualys normalized values.
debugData	url	requestUrl	/api/1/internal/app/activedirectory/0oa14wmiz0OSLKEKLUIZ/agent/a531g5al30panDIWK0h8/actionResult?responseId=7e563856-af57-45a1-8a10-2e173812c681	URL Requested in the event log
transaction	id	baseEventId	X1m4XfJiSORl5BoaoWinvQAAAbQ	Unique identifier for this transaction.
Attribute	uuid	deviceEventId	ca29ae85-f325-11ea-9172-292a8c71fec7	Unique identifier for an individual event

Object Type	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Attribute	version	version	0	Versioning indicator
target	id	destination UserId	0oa14wmiz0OS LKEKLUIZ	ID of a target
target	type	targetType	AppInstance	Type of a target - AppInstance, AppUser, User, PolicyRule, PolicyEntity
target	alternateId	destination User	abc.company.com	Alternative id of a target

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	IAM
deviceModel	
deviceVendor	Okta
deviceHost	prismvmXX2
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 09, 2021 11:29:04 PM

Field Value Mappings

Data source field: outcome

Source Values	Qualys Normalized Values
SUCCESS	Success
FAILURE	Failure
SKIPPED	Skipped
ALLOW	Allow
DENY	Deny
CHALLENGE	Challenge
UNKNOWN	Unknown

Data source field: deviceSeverity

Source Values	Qualys Normalized Values
DEBUG	Debug
INFO	Informational
WARN	Warning
ERROR	Error