



Qualys Context Extended Detection and Response

Microsoft Azure AD

Data Mapping Guides

January 22, 2023

Copyright 2023 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	4
About Qualys.....	4
Qualys Support	4
Overview	5
Device Details.....	5
Supported Formats	5
Data Field Mappings	6
Qualys Internal Fields	11

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 heterogeneous 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 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 Microsoft Azure Active Directory (AD) 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** – Cloud Infrastructure
- **Device Vendor** – Microsoft
- **Device Product** – Microsoft Active Directory
- **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 Microsoft Active Directory using the following formats:

- **JSON**

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 – Active Directory

deviceVendor – Microsoft

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
category/metadatas	eventName	RoleManagement/AzureADSignIns	Brief standard meaning of the message easy to read for Analyst
result/errorCode	outcome	success	Outcome of the event
resultReason/failureReason	reason	Microsoft.Online.DirectoryServices.DirectoryValueNotFoundException	Reason for the audit event log to occur.
activityDisplayName	eventType	Triggered PIM alert	Type of the event.
activityDateTime/createdDateTime	eventTime	2022-03-09T20:25:40.1332226Z, 2022-03-09T20:42:10Z	Date and time (UTC) the sign-in was initiated.
loggedByService	sourceServiceName	PIM/Core Directory	Service name on the source machine(the machine who has generated this event as per the log audit)
operationType	eventSubType	ActivateAlert	SubType of the event associated with EventType field.
displayName / appDisplayName	application	Azure Credential Configuration Endpoint Service, Microsoft Azure Signup Portal	App name displayed in the Azure Portal.
servicePrincipalName	application	Microsoft Approval Management	Name of the application used
id/ userId	sourceUserId	86729171-9d9c-47e2-a3ec-1c646a77a824	User principal name of the user that initiated the sign-in.
userPrincipalName	sourceUser	qualysthreatsandbox@08bvt.onmicrosoft.com	ID of the user that initiated the sign-in.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
ipAddress	sourceIpV4	20.190.132.106	IP address of the client used to sign in.
displayName	object	Azure AD Directory Roles	Name of the policy
type	objectCategory	Other/Policy	URL categorization of the URL in event log. (Primarily used for URL categorization)
userPrincipalName	destination user	null	Username using/logged-in the destination machine(the username present in the log audit as per the log audit logged by the device)
displayName/applied Conditional AccessPolicies	customArray1	AccountEnabled	Indicates the property name of the target attribute that was changed.
oldValue	customArray2	null	Indicates the previous value (before the update) for the property.
newValue	customArray3	TRUE	Indicates the updated value for the property.
id	externalId	01e6c214-37c6-4c30-84bc-35c1f2cc9001	Unique ID representing the sign-in activity.
userDisplayName	-	Adam Joe	Display name of the user that initiated the sign-in.
appId	-	8e0e8db5-b713-4e91-98e6-470fed0aa4c2	Unique GUID representing the app ID in the Azure Active Directory
clientAppUsed	userAgent	Browser	Identifies the client used for the sign-in activity.
correlationId	-	c90515af-9688-4374-b815-837a4238b15a	The request ID sent from the client when the sign-in is initiated; used to troubleshoot sign-in activity.
conditionalAccessStatus	-	notApplied	Reports status of an activated conditional access policy. Possible values are: success, failure,

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
			notApplied, and unknownFutureValue.
isInteractive	customString6	TRUE	Indicates if a sign-in is interactive or not.
riskDetail	customString7	none	Provides the 'reason' behind a specific state of a risky user, sign-in or a risk event. The possible values are: none, adminGeneratedTemporaryPassword, userPerformedSecuredPasswordChange, userPerformedSecuredPasswordReset, adminConfirmedSigninSafe, aiConfirmedSigninSafe, userPassedMFA DrivenByRiskBasedPolicy, adminDismissedAllRiskForUser, adminConfirmedSigninCompromised, unknownFutureValue. The value none means that no action has been performed on the user or sign-in so far.
riskLevelAggregated	riskScore	none	Aggregated risk level. The possible values are: none, low, medium, high, hidden, and unknownFutureValue. The value hidden means the user or sign-in was not enabled for Azure AD Identity Protection.
riskLevelDuringSignIn	-	none	Risk level during sign-in. The possible values are: none, low, medium, high, hidden, and unknownFutureValue. The value hidden means the user or sign-in was not enabled for Azure AD Identity Protection.
riskState	customString8	none	Reports status of the risky user, sign-in, or a risk event. The possible values are: none, confirmedSafe, remediated, dismissed, atRisk, confirmedCompromised, unknownFutureValue.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
riskEventTypes	customString9	maliciousIPAddress	Risk event types associated with the sign-in. The possible values are: unlikelyTravel, anonymizedIPAddress, maliciousIPAddress, unfamiliarFeatures, malwareInfectedIPAddress, suspiciousIPAddress, leakedCredentials, investigationsThreatIntelligence, generic, and unknownFutureValue.
resourceDisplayName	customString10	Microsoft Graph	Name of the resource the user signed into.
resourceId	-	00000003-0000-0000-c000-000000000000	ID of the resource that the user signed into.
additionalDetails	message	MFA requirement satisfied by claim in the token	Provides additional details on the sign-in activity
deviceId	deviceId		Refers to the UniqueID of the device used for signing in.
displayName	deviceName		Refers to the name of the device used for signing in.
operatingSystem	osDetails	MacOs	Indicates the operating system name and version used for signing in.
browser	userAgent	Chrome 98.0.4758	Indicates the browser information of the used for signing in.
isCompliant	customString11	FALSE	Indicates whether the device is compliant.
isManaged	customString12	FALSE	Indicates whether the device is managed.
trustType	customString13	Workplace Joined	Provides information about whether the signed-in device is Workplace Joined, AzureAD Joined, Domain Joined.
city	geoSourceCity	Hayward	Provides the city where the sign-in originated. This is calculated using latitude/longitude information from the sign-in activity.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
state	-	California	Provides the State where the sign-in originated. This is calculated using latitude/longitude information from the sign-in activity.
countryOrRegion	geoSourceCountry	US	Provides the country code info (2 letter code) where the sign-in originated. This is calculated using latitude/longitude information from the sign-in activity.
geoCoordinates	geoSourceCoordinates	**	Provides the latitude, longitude and altitude where the sign-in originated.
altitude	-	1024.13	The altitude (height), in feet, above sea level for the item.
latitude	-	37.63243	The latitude, in decimal, for the item.
longitude	-	-122.0812	The longitude, in decimal, for the item.
id	-	SecurityDefaults	An identifier of the conditional access policy
displayName	-	Security Defaults	Refers to the Name of the conditional access policy (example: "Require MFA for Salesforce").
result	-	success	Indicates the result of the CA policy that was triggered. Possible values are: success, failure, notApplied (Policy isn't applied because policy conditions were not met),notEnabled (This is due to the policy in disabled state), unknown, unknownFutureValue.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	Cloud Infrastructure
DeviceModel	Azure Active Directory
DeviceVendor	Microsoft
DeviceHost	-
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