Qualys Extended Detection and Response

Cisco Duo IAM

Data Mapping Guide

February 16, 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 Duo 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 Duo IAM
- **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 Cisco Duo IAM using the following formats:

- **JSON**

For information on configuring collectors, refer to the Deploying a Collector 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

EventTypes Admin Logs

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
action	eventType	admin_login	The type of change that was performed.
description	description		String detailing what changed, either as free-form text or serialized JSON. When the description contains JSON it may be either a serialized object or a serialized array of objects. Each key in the object(s) corresponds to a property that was changed. This JSON is intended only to summarize the change, not to be de-serialized. The first example below is for a “user_update” action. The object that changed was a user whose Duo username is “jsmith”. The change saved new values for the user’s “notes” and “realname” fields, overwriting the previous values if any were set. They correspond to the similarly named fields in the Modify User call in the Admin API and the User Details page in the Admin Panel. The second example shows an “admin_login_error” action. The administrator's login attempt failed because the admin attempted to use SSO but, as indicated by the “error” in the description, SAML login is disabled for administrators on that account.
description.ip_address	destinationIpv4	64.39.96.133	IPv4 address of the destination machine (the machine who has generated this event as per the log audit)
description.email	destinationUser	johndoe@company.com	Username using/logged-in the destination machine (the username present in the log audit as per the log audit logged by the device)
description.phone	phoneNumber	16508016200	
description.enroll_policy	policy	Require Enrollment	Policyname/rulename from the device
description.groups.name	group	sec-DuoTest	Group Name to which entity (asset/user) in audit log belong

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
description.status	outcome	Disabled	Outcome of the event
description.type	application	Mobile	Name of the application used
description.platform	osDetails	iOS	OS Information of the asset
description.number	phoneNumber	16502817037	
description.enrollment_email_body	message	Qualys IT has requested that you enroll with Duo Security\'s two-factor authentication service. Just click this link to begin the enrollment process:\\r\\n\\r\\n<enrollment-link>\\r\\n\\r\\nYou should have already received an email from IT Help (Subject: Duo 2 Factor) with instructions for setup on both Android & IOS. That document can also be found here:\\r\\n\\r\\nhttps://drive.google.com/a/cisco.com/folderview?id=0B-F7nL31yu_GfkRpb2VKNHNGOElHblBjZWhLOVZJdUcxa3kzbUs4bWIzNDdrY2lLWVlVblk&usp=sharing\\r\\n\\r\\n Please contact ITHelp@cisco.com if you need assistance or have any questions.	Additional field - future use
isotimestamp	eventTime	2014-09-22T20:11:32+00:00	ISO8601 timestamp of the event.
object	object	Generic Smartphone	The object that was acted on. For example: “jsmith” (for users), “(555) 713-6275 x456” (for phones), or “HOTP 8-digit 123456” (for tokens).

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
username	sourceUser	Admin	The full name of the administrator who performed the action in the Duo Admin Panel. If the action was performed with the API this will be “API”. Automatic actions like deletion of inactive users have “System” for the username. Changes synchronized from Directory Sync will have a username of the form (example) “AD Sync: name of directory.”
host	destinationHost	api-c25edaaa.duosecurity.com	The host name of the system where Duo Windows Logon is installed.
EventName	eventName	EventType descriptions: https://duo.com/docs/adminapi	Brief standard meaning of the message easy to read for Analyst

Authentication Logs

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
action	eventType	admin_login	The type of change that was performed.
description	description		String detailing what changed, either as free-form text or serialized JSON. When the description contains JSON it may be either a serialized object or a serialized array of objects. Each key in the object(s) corresponds to a property that was changed. This JSON is intended only to summarize the change, not to be de-serialized. The first example below is for a “user_update” action. The object that changed was a user whose Duo username is “jsmith”. The change saved new values for the user’s “notes” and “realname” fields, overwriting the previous values if any were set. They correspond to the similarly named fields in the Modify User call in the Admin API and the User Details page in the Admin Panel. The second example shows an “admin_login_error” action. The administrator's login attempt failed because the admin attempted to use SSO but, as indicated by the “error” in the description, SAML login is disabled for administrators on that account.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
description.ip_address	destinationIpv4	64.39.96.133	IPv4 address of the destination machine (the machine who has generated this event as per the log audit)
description.email	destinationUser	johndoe@company.com	Username using/logged-in the destination machine (the username present in the log audit as per the log audit logged by the device)
description.phone	phoneNumber	16508016200	
description.enroll_policy	policy	Require Enrollment	Policyname/rulename from the device
description.groups.name	group	sec-DuoTest	Group Name to which entity(asset/user) in audit log belong
description.status	outcome	Disabled	Outcome of the event
description.type	application	Mobile	Name of the application used
description.platform	osDetails	iOS	OS Information of the asset
description.number	phoneNumber	16502817037	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
description.enrollment_email_body	message	Qualys IT has requested that you enroll with Duo Security\'s two-factor authentication service. Just click this link to begin the enrollment process:\\r\\n\\r\\n<enrollment-link>\\r\\n\\r\\nYou should have already received an email from IT Help (Subject: Duo 2 Factor) with instructions for setup on both Android & IOS. That document can also be found here:\\r\\n\\r\\nhttps://drive.google.com/a/cisco.com/folderview?id=0B-F7nL31yu_GfkRpb2VKNHNGOElHblBjZWhLOVZJdUcxa3kzbUs4bWIzNDdrY2lLWVlVblk&usp=sharing\\r\\n\\r\\nPlease contact ITHelp@cisco.com if you need assistance or have any questions.	Additional field - future use
isotimestamp	eventTime	2014-09-22T20:11:32+00:00	ISO8601 timestamp of the event.
object	object	Generic Smartphone	The object that was acted on. For example: “jsmith” (for users), “(555) 713-6275 x456” (for phones), or “HOTP 8-digit 123456” (for tokens).
username	sourceUser	Admin	The full name of the administrator who performed the action in the Duo Admin Panel. If the action was performed with the API this will be “API”. Automatic actions like deletion of inactive users have “System” for the username. Changes synchronized from Directory Sync will have a username of the form (example) “AD Sync: name of directory.” The type of activity logged. one of: “authentication” or “enrollment”.
host	destinationHost	api-c25edaaa.duosecurity.com	The host name of the system where Duo Windows Logon is installed.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
EventName	eventName	EventType descriptions: https://duo.com/docs/adminapi	Brief standard meaning of the message easy to read for Analyst

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	IAM
deviceModel	Duo
deviceVendor	Cisco
deviceHost	el.xyz.com
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

Field Value Mappings

Source Values	Qualys Normalized Values
SUCCESS	Success
FAILURE	Failure
Enabled	Enabled
Disabled	Disabled
Active	Active
Bypass	Bypass