



Qualys Context XDR v1.x

Release Notes

Version 1.0.4

April 26, 2022

Here's what's new in Qualys Context XDR 1.0.4!

[Support for Linux Cloud Agent Profile](#)

[Newly Added Assets Tab](#)

[New Improvement for Threat Intel Enrichment for URLs](#)

[Onboarded Azure Active Directory Collector](#)

Context XDR 1.0.4 brings you more improvements and updates!

Support for Linux Cloud Agent Profile

With this release, we have now added support of Cloud Agent Profile for Linux agents. You can now create a Cloud Agent Profile for Linux OS to define what logs you want to collect from hosts, where you want to collect them, and the assets you want to collect from.

Kindly note that, Context XDR only supports for Linux agents with version 4.9 or above.

Navigate to **Configuration > Cloud Agent Profiles > Profiles** and click **New Profile**. Enter the basic details for Name and Description of profile and select **Linux** as the Operating System and proceed to next steps for configuration till step 5.

The screenshot shows the 'New Profile' configuration page. On the left, a sidebar lists the steps: 1. Basic Detail (selected), 2. Log Collection Details, 3. Destination Details, 4. Default Rules, and 5. Assign Assets. The main form area is titled 'Profile Basic Details' and contains the following fields:

- Name ***: Text input field containing 'Test_Profile'.
- Description**: Text area containing 'Demo'.
- Operating System ***: Dropdown menu with 'Linux' selected. This field is highlighted with a red rectangular box.

At the bottom of the form are two buttons: 'Cancel' and 'Next'.

After the profile is successfully saved. You can view the status as **Created** on the Profiles tab. When the profile is created, Qualys Cloud Agents starts to collect logs from the assets you selected and forwards them to the destination you configured.

The screenshot shows the 'Cloud Agent Profiles' table in the Qualys console. The table has the following columns: STATUS, PROFILE NAME, DESTINATION, OPERATING SYSTEM, CREATED BY, and CREATED ON. The 'STATUS' column is highlighted with a red box, and the value 'Created' is visible in the first row. The table contains two rows of data:

STATUS	PROFILE NAME	DESTINATION	OPERATING SYSTEM	CREATED BY	CREATED ON
Created	Events by tag	Context XDR	Linux	[Redacted]	Apr 14, 2022 08:01 pm
Created	sfd	Context XDR	Linux	[Redacted]	Apr 20, 2022 11:15 am

Newly Added Assets Tab

We have introduced a new **Assets** tab under **Cloud Agent Profiles** of configuration. The **Assets** tab displays the list of all configured assets in detailed status. You can view the complete details for XDR status, Manifest status, Profile, etc. for each asset.

XDR STATUS	AGENT UUID	MANIFEST STATUS	UPDATED ON	OS	PROFILES	TAGS
●	[blurred]	Manifest Assigned	Apr 16, 2022 12:41 pm	Microsoft Windows Server 201...	Test_profile 1 more	Cloud Agent
●	[blurred]	Manifest Assigned	Apr 16, 2022 12:41 pm	Windows Microsoft Windows S...	Test_profile 1 more	XDR Cloud Agent
●	[blurred]	Manifest Assigned	Apr 16, 2022 02:03 am	Windows Microsoft Windows S...	-	Cloud Agent
●	[blurred]	Manifest Assigned	Apr 14, 2022 08:36 pm	CentOS Linux 7.0.1406 (Core) ...	Verify...	Linux_New_Tag Cloud Agent
●	[blurred]	Manifest Assigned	Apr 14, 2022 08:36 pm	Red Hat Enterprise Linux Serve...	Verify...	Linux_New_Tag Cloud Agent
●	[blurred]	Manifest Assigned	Apr 14, 2022 08:01 pm	CentOS Linux 8.0.1905 (Core) ...	Events by tag 1 more	Cloud Agent
●	[blurred]	Manifest Assigned	Apr 14, 2022 08:01 pm	Red Hat Enterprise Linux 8.5 (O...	Events by tag 1 more	Cloud Agent
●	[blurred]	Manifest Assigned	Apr 14, 2022 08:01 pm	CentOS Linux 8.5.2111 8.5.2111	Events by tag	Cloud Agent

The detailed description of each status is given below:

XDR Status - Displays the Context XDR application is activated for an asset or not.

Agent UUID - Click Agent UUID to view the complete summary details of the selected asset.

Manifest Status - Displays the status of a manifest for an asset.

Updated On - Displays the date and time of the last activity on the asset.

OS - Displays the operating system associated with the asset.

Profiles - Displays the profiles associated with the asset.

Tags - Displays the tags associated with the asset.

New Improvement for Threat Intel Enrichment for URLs

With this release, you can view the enrichment of device logs with the threat intel URL feeds. The device audit logs for URLs gets correlated with the threat feed URLs and Qualys threat feed enrichment can be viewed on UI in case malicious URLs is viewed in the logs.

You can navigate to **Threat Management > Events** tab to view the detected history of event logs. Then, use search tokens filter with `'threatIntelFlagmatch: true and ThreatIntelType: URL'` to view the events that are corelated and matched with the Threat Intel feeds. This helps the security analyst to narrow down the threat detection process to specific threat actors.

The screenshot shows the 'Events' tab in the Threat Management interface. A search filter is applied: `threatIntelFlagmatch:true and threatIntelType:URL`. The search results show a bar chart for the month of April. Below the chart, the event details for '2022-04-23 11:42 PM' are displayed. The event source is 'Cisco Umbrella' and the event type is 'proxylogs'. The event details include: `sourceIpV4: 10.3.15.100`, `destinationIpV4: [redacted]`, `action: Allow`, `collectorId: [redacted]`, `collectorReceivedTime: 2022-04-23 11:55 PM`, `deviceModel: Umbrella`, `deviceType: Proxy`, `deviceVendor: Cisco`, `eventContext: local-to-remote`, `eventId: 101e5e47-c9e6-4201-9ac4-f81f8a996764`, `eventSourceId: 39ada2bb-bf11-411b-bc76-92705129891a`, `eventSourceName: Cisco umbrellla 25 March_eventSource`, `eventTime: 2022-04-23 11:42 PM`, `eventType: proxylogs`, `natSourceIP: 80.227.210.150`, `objectCategory: Advertisements,Business Services,Application`, `proxyBlockedCategories: Anyconnect Roaming Client`, `requestUrl: https://redirect.viglink.com/`, `sourceHost: 131329-T480`, `status: 302`, `tags: Proxy`. The event details also show: `threatIntelFlagMatch: true`, `threatIntelReason: PhishTank`, `geoDestinationCity: Dublin`, `geoDestinationCoordinates: 53.3338,6.2488`, `geoDestinationCountry: Ireland`, `threatIntelSource: Threat Connect`, and `threatIntelType: URL`. The 'EVENT VALUES (25)' and 'QUALYS ENRICHED VALUES (7)' sections are visible, with the latter containing the following values: `geoDestinationCity: Dublin`, `geoDestinationCoordinates: 53.3338,6.2488`, `geoDestinationCountry: Ireland`, `threatIntelFlagMatch: true`, `threatIntelReason: PhishTank`, `threatIntelSource: Threat Connect`, and `threatIntelType: URL`.

Onboarded Azure Active Directory Collector

We now support Azure Active Directory cloud collector that allows you to collect all the user attributes/data into Context XDR to enrich data from other log sources.

Navigate to **Configuration > Data Collection > Catalog**. Navigate to the Microsoft Azure Active Directory tile and click **Configure Cloud Azure Active Directory**. Enter the required details to configure the Azure Active Directory collector and save. Once the collector binds successfully, the collector status appears as Active under the Sources tab.

The screenshot shows the 'Configuration' page in the XDR interface, specifically the 'Data Collection' section. The 'Catalog' tab is selected, showing a grid of data sources. The 'Sources' tab is active, displaying a list of configured sources. The 'Microsoft Azure Active Directory' source is highlighted, and the 'Configure Cloud Azure Active Directory' button is visible. The 'Sources' tab shows a total of 48 sources. The 'Catalog' tab shows a list of sources, including Akamai, Arbor-APS, Microsoft Azure Active Directory, Blue Coat, Check Point Firewall, Check Point IPS, Cisco Endpoint, Cisco IPS, and Cisco IAM. The 'Microsoft Azure Active Directory' source is listed as '1 Configured'.